The Report of the University of California Campus Security Task Force

Table of Contents

UC CAMPUS SECURITY TASK FORCE MEMBERSHIP

Members

W. Rory Hume, Co-Chair
Provost and Executive Vice President - Academic and Health Affairs
University of California, Office of the President

Katherine Lapp, Co-Chair
Executive Vice President - Business Operations
University of California, Office of the President

Benjamin Allen
2007-08 Student Regent (law student, Berkeley campus)

David Birnbaum
University Counsel
Office of the General Counsel

Linda F. Bisson
Professor, Viticulture and Enology, and
Division Chair, UC Davis Academic Senate
University of California, Davis

Greg Cendana
Student Representative (undergraduate, UCLA)

Bob Charbonneau
UCOP Emergency Manager
University of California, Office of the President

Mary Croughan
Professor of Obstetrics, Gynecology, and Reproductive Sciences
Mt Zion Hospital
University of California, San Francisco

Joel E. Dimsdale
Professor of Psychiatry, and
Co-Chair, UC Student Mental Health Oversight Committee
University of California, San Diego

Kristine Hafner
Associate Vice President
Information Resources and Communications
University of California, Office of the President

Victoria L. Harrison
Police Chief
University of California, Berkeley

Paul Henisey
Police Chief
University of California, Irvine

Valerie Lucus
Emergency Manager
University of California, Davis

Janina Montero
Vice Chancellor – Student Affairs
University of California, Los Angeles

John Oakley
Academic Council Chair, 2006-07
University of California, Office of the President

Karl Ross
UCLA Police Chief, and
Chief of the Council of UC Police Chiefs
University of California, Los Angeles

Judy Sakaki
Vice President – Student Affairs
University of California, Office of the President

Thomas Vani
Vice Chancellor –
Business and Administrative Services
University of California, Santa Cruz

Michael Young
Vice Chancellor – Student Affairs, and
Co-Chair, UC Student Mental Health Oversight Committee
University of California, Santa Barbara

Staff

Bob Charbonneau, Task Force Staff
UCOP Emergency Manager
University of California, Office of the President

Clint Haden, Task Force Staff
Director of Campus Life - Student Affairs
University of California, Office of the President

Valery Oehler, Task Force Staff
Associate Director of Campus Life - Student Affairs
University of California, Office of the President

Gail Riley, Task Force Staff (principal)
Director of Legislation
Police Services Coordination -
Business Operations
University of California, Office of the President

Executive Summary

Preface

There is no greater priority for the University of California system than the safety and security of students, faculty, staff, and visitors. The impact of the tragic shootings at Virginia Tech that occurred on April 16, 2007 continues to be felt across the nation and has altered our collective awareness of the adequacy of security at the nation's institutions of higher education. This awareness is grounded in the universal understanding that, given a different conjunction of circumstances, what happened at Virginia Tech that day *could* have happened elsewhere, including at the University of California.

The Chancellor of each UC campus is responsible for the public safety of the campus. The Campus Security Task Force was charged to assess public safety capabilities at the campuses.

The University can take pride in the many positive and pro-active actions that it has already taken over the last few years to ensure the safety and security of the entire campus community. For instance, the University has been actively preparing and training to respond to an "active shooter" event since well before Virginia Tech. University Police have been preparing to rapidly respond to such an incident through extensive tactical firearms and active shooter scenario training exercises, oftentimes in conjunction with other local law enforcement and public safety agencies. Most campuses have established interoperable radio communications capability with their local mutual aid agencies. Campus-wide educational and awareness programs and procedures on how to respond to an active shooter, shelter in place, or evacuate the campus have been developed and incorporated into emergency plans. Every campus already has some type of emergency mass notification system in place.

In order to reduce the threat of workplace violence, most campuses have comprehensive workplace violence prevention and response programs that include multi-disciplinary behavioral threat management teams. Campuses provide workplace violence training and education for staff, supervisors, faculty, and students. These programs typically cover prevention, early detection and intervention, conflict resolution/mediation, supervisory response, policies, referral/response procedures, and anger/stress management, as well as general personal safety and security. A number of administrative, management, supervisory controls, policies, and procedures are already in place to prevent, assess, mitigate, and respond to potential workplace violence. Campuses have also implemented a number of physical security measures and safeguards such as building access controls, surveillance systems, panic or alarm systems, and emergency call boxes.

On the student mental health front, UC has targeted a dedicated 3% increase to the University Registration Fee (one of only two Universitywide fees that all enrolled students must pay) for 2007-08 specifically to address student mental health needs. Examples of the uses of this additional revenue by campuses include the hiring of additional mental health services staff, the augmentation of mental health staff salaries, new training and outreach models, and increased resources for programs dedicated to prevention and intervention.

However, despite this pro-active record of recent accomplishments outlined immediately above, it became clear to the Task Force during the course of its review that much can be done, including the full funding and implementation of the recommendations of prior University Committees that have already concluded their work in the areas of student mental health and hazard vulnerability assessment. Following is a thematic summary of the findings and recommendations of the three Workgroups established by the Task Force (focusing respectively on Student Mental Health, Crisis Communication and Emergency Preparedness, and Campus Safety) to examine the safety and security of University of California campuses.

Student Mental Health

As underscored by the findings and recommendations of the UC Student Mental Health Committee Final Report (See Appendix C) issued in September 2006, providing a broad array of campus student support services and student life opportunities is critical to creating healthier campus communities. A well-funded, robust, comprehensive, and interconnected network of specifically student-mental-health related services is the first and best line of defense in facilitating the early identification and treatment of students presenting mental-health-related behavioral issues. These front-line services can be complemented by the ready availability of an appropriately responsive array of other campus programs and services focusing on prevention, intervention, and education.

Even with such programs and services in place, campus administrators encounter a range of obstacles in navigating the maze of federal and state privacy laws and internal UC policies in their efforts either to share information with colleagues about students exhibiting severe psychological behaviors, or to address those behaviors responsibly in a way that balances the rights of the individual student with considerations of public safety.

UC campuses have in place multidisciplinary behavioral management teams and associated highly developed crisis management/response protocols to help ensure that accurate, efficient, and rapid communication occurs across campus units during a crisis that potentially threatens student and campus safety. But on-the-ground communication and information-sharing regarding the at-risk behavior of students may be compromised by confusion resulting from the inherent complexities of interconnected state and federal privacy laws. Differing and not universally well-understood legal constraints on the sharing of student information apply, depending on the specific functional roles of individual campus administrators. Moreover, the inevitable attrition of staff over time necessitates sustained training and education efforts to ensure that all staff is kept current on the institution's communication protocols.

Recommendations:

- The University should continue efforts to implement program improvements identified in the "Plan of Action for Creating Healthier Campus Learning Communities," outlined in the UC Student Mental Health Report (Appendix C). Campuses will build implementation plans based on the Provisional Campus Blueprint for Implementation of the Report Recommendations (Appendix D) to enable quick implementation as funding becomes available.

- Each campus should ensure that a multidisciplinary behavioral management team (or coordinated series of teams) has been established to address issues, problems or students, staff, or faculty who may pose a threat to the campus community. These teams should inform the campus community of their function and purpose and provide appropriate training to that community. For teams already in place, an immediate review of the current structure, composition, and related protocols of the team should be undertaken with special reference to the scope, adequacy, accuracy, and effectiveness of its communication and information-sharing mechanisms as they relate to students.

- The University should immediately undertake a formal examination (with full opportunity for comment by all segments of the University community) of the impacts of specific proposed changes to student and patient privacy and related laws, as well as to its own internal policies, from the perspective of balancing individual rights with public safety needs.

- The Office of the General Counsel should continue to maintain among its legal staff an attorney specifically trained in the area of mental health-related law to serve as a student mental health resource for the campuses. In addition, that Office should prepare and make available concise written systemwide legal guidelines and other reference materials that delineate how, with whom, and for what purposes information regarding students exhibiting student-mental-health-related behaviors can be shared.

- The Office of the President, in coordination with the Office of the General Counsel, should initiate the development of regular information-sharing and communications training programs that involve key campus partners and that are informed by a common set of systemwide disclosure standards and communications protocols regulating the sharing of sensitive information about students.

Emergency Communications

The Virginia Tech shootings highlighted the importance of effective and timely communications when responding to a violent critical incident. Every campus should be able to expeditiously communicate both internally to the entire campus community, and externally with its local public safety mutual aid and emergency services providers. Whenever possible, each campus dispatch center should have enhanced-911 capability to directly receive wireless emergency calls originating from the campus. Every campus currently has some type of mass notification system in place. Most commonly these include broadcast email and voicemail messages to campus accounts or phones, webpage banners or links, emergency hotlines or call-in numbers, and mobile public address systems in public safety vehicles. Mass notification systems should be both layered and redundant – no single means of communications should be solely relied upon to reach the entire campus community.

Recommendations:

- **Emergency Mass Notification Systems:** Each campus should complete a 'Gap Analysis' which inventories and evaluates current emergency communications practices, capabilities, and needs with the objective of identifying and closing any gaps.

- **Crisis Communication:** Each campus should develop an interdisciplinary team and Crisis Communication Plan that clearly defines roles and responsibilities as well as delegations and lines of authority for various campus officials to support timely campus-wide warning and notification during an emergency situation or critical incident.

- **Emergency Communications:** Ideally, each campus should establish communications interoperability with its immediate mutual aid and emergency services providers. Such capacity would include the ability to communicate directly with police, fire and emergency medical services from surrounding agencies in order to coordinate response to a critical incident. An assessment of how to fund communications interoperability should be undertaken by the campuses.

Preparedness and Response

Campuses should ensure they have adequate and specific plans, procedures, resources and training to rapidly and effectively respond to a violent critical incident.

In 2004, the University voluntarily adopted the National Preparedness Standard on Disaster and Emergency Management and Business Continuity Programs (NFPA/ANSI) as the basis for its annual systemwide programmatic benchmarking survey of its emergency management programs. All campuses and medical centers annually report to the Office of the President on their status and progress in implementing their programs. The Office of the President then prepares an annual systemwide status report for senior University management. The comprehensive national standard represents the highest measure against which University emergency preparedness is continually gauged.

Recommendations:

- **Personnel & Equipment Resources:** Each campus should assess its public safety responder staffing levels and equipment to determine whether it has the resources required to provide a rapid and effective initial response to a violent critical incident.

- **Personnel & Equipment Resources:** Each campus should develop an 'active shooter' response training plan that includes mutual aid emergency responders. Campus-wide emergency preparedness awareness and educational programs should include appropriate response to an 'active shooter' incident, sheltering in place, and evacuation procedures.

- **Emergency Preparedness:** Each campus should work towards full compliance with the National Preparedness Standard particularly using the Incident Command System (ICS), establishing and testing campus-wide notification and alerting systems, developing standard operating procedures for responding to all types of incidents, and conducting annual exercises, evaluations, and corrective actions.

- **Policies & Procedures:** Consistent with the National Preparedness Standard, each campus should have in place procedures to address:

    Active shooter response
    Hostage/barricaded suspect
    Use of force
    Evacuation of campus facilities
    Access controls
    Sheltering in place
    Threat management
    Timely alerting and warning
    Major incident notifications

Prevention and Hazard Mitigation

The Hazard Vulnerability Assessment (HVA) report, completed at the direction of the systemwide Safety, Security and Anti-Terrorism Committee in 2005, included recommended mitigation measures for threat events including 'active shooter' and related 'workplace violence'. Recommendations included training and equipping the University Police Departments to rapidly respond to such incidents, review of campus security plans and measures, and security surveys at high-risk office locations.

Recommendations:

- **Facilities & Infrastructure:** Security surveys should be conducted on existing campus buildings and should include security recommendations, as necessary, for further evaluation, selection, and prioritization by the campus. Design review for all new buildings should include an assessment of the building and recommendations to enhance building security.

- Each campus should continue to develop an overall campus hazard mitigation strategy based upon its own institutional priorities, operational experience, and cost-benefit analysis.

End of Executive Summary

Report of the UC Campus Security Task Force

Introduction

Among the University's many recent actions to provide greater campus security, foremost are major self-assessments of its vulnerability to hazards (broadly defined to include all types of physical threats) and the current state of its campus student mental health and related services. These self-assessments have resulted in new policy (the Policy on Safeguards, Security, and Emergency Management (http://www.ucop.edu/facil/pd/emergprep/ssempolicy.pdf).
issued in January 2006) as well as in a major new report on its student mental health services and related programs needs (the Student Mental Health Committee Final Report, issued in September 2006 (See Appendix C).

Both efforts have significantly informed the content of the UC Campus Security Task Force Report, which also considers and benefits from the recommendations included in the Virginia Tech internal working group reports and the report of the review panel established by the Governor of Virginia, as well as other state and federal reports related to the Virginia Tech incident (See Appendix B).

Student Mental Health Needs Assessment

In December 2005, University President Robert C. Dynes and Provost Wyatt R. Hume established the UC Student Mental Health Committee to "study student mental health issues within the University." The Committee's findings, issued in its Final Report that was presented to the UC Board of Regents in September 2006, portrayed a "stark new reality" of student mental health-related needs that has grown dramatically both in frequency and severity in recent years and that is putting significant stress on the University's services and programs in this area. The Report called for "aggressive intervention" on the part of the University that "must include a systematic review of policy, enhanced communication mechanisms, and a renewed commitment to campus-wide collaboration along with an infusion of new resources commensurate with both the nature and magnitude of the challenge now facing the University."

The Report also presented a specific "Plan of Action for Creating Healthier Campus Learning Communities", organized in three Tiers from immediate student mental health counseling services and related needs to targeted intervention programs for particularly vulnerable populations and on to a broader base of preventative efforts engaging the entire campus community. The University is currently in the process of developing a funding Plan to actualize the critically important Student Mental Health Final Report recommendations at each of its ten campuses.

Hazard Vulnerability Assessment

In 2003, the University established the systemwide Safety, Security and Anti-Terrorism (SSAT) Committee to assess the University's overall security and vulnerability to all types of physical threats including natural hazards, technological hazards, terrorist acts, and human-caused events

such as the Virginia Tech 'active shooter' incident. Following the hazard vulnerability assessment process, the University issued a new Policy on Safeguards, Security, and Emergency Management [http://www.ucop.edu/facil/pd/emergprep/ssempolicy.pdf].

Each campus and the Office of the President are required to maintain comprehensive and effective programs encompassing risk assessment and mitigation, emergency preparedness and response, and business recovery to strengthen crisis and consequence management capabilities across the University system. Each Chancellor is responsible for implementation at his or her respective campus, and has designated one or more responsible officials with full authority to implement campus-wide safeguards, security, and emergency management programs.

Composition and Methodology of the Task Force

Immediately after the Virginia Tech shootings, UC convened the campus Police Chiefs, Vice Chancellors of Student Affairs and other relevant university officials to explore the full range of issues evident in the shootings: campus security measures, student mental health practices and policies, mass notification capabilities, emergency preparedness, and related legal issues regarding each. As a result of that preliminary review, President Dynes concluded that while UC has many sound policies and practices in place, much can be done.

President Dynes therefore created the UC Campus Security Task Force to "…study how campuses can enhance their security, notification processes, mental health services, and general preparedness," and appointed Provost and Executive Vice President for Academic Affairs Wyatt R. Hume and Executive Vice President of Business Operations Katherine Lapp to serve as Co-Chairs. The Task Force membership represents all elements of the campus community, including the Chair of the UC Council of Police Chiefs and Police Chiefs from two other campuses, the Chair of the Academic Senate, representatives of the Vice Chancellors of Administration, campus Emergency Managers, Vice Chancellors of Student Affairs, and the Vice President of Student Affairs at the Office of the President.

The Task Force decided to review three principal areas – student mental health, campus safety, and crisis communication and emergency preparedness – and created Workgroups to address each. These three subjects reflect the Task Force analysis of the central issues in the Virginia Tech shootings. Most other review commissions established to examine the shootings have focused the bulk of their attention on these same three subject areas (See Appendix B).

The Workgroups focused their attention on identifying gaps or enhancements necessary to ensure that the entire University community is afforded the greatest protection available.

Funding of the Task Force Recommendations

The Campus Security Task Force recognizes that each campus is unique and that each has its own priorities. The Task Force further understands that competing funding priorities compel each campus to determine for itself which Task Force recommendations are both necessary and feasible for that particular campus. Although declining state resources have made it difficult to fund all elements of the University's mission, the University's Board of Regents has already

made a commitment to fund campus student mental health needs (see below). In addition, opportunities are being evaluated through the Office of the President's Risk Services unit to address other recommendations of the Task Force.

Funding of Campus Student Mental Health Needs

Shortly following presentation of the Student Mental Health Committee's Final Report to the Board of Regents in September 2006, the Vice Chancellors for Student Affairs of each of the University's ten campuses made a collective recommendation to the Provost for the level of funding that would be required to implement the most critical components of the Final Report: approximately $41 million in permanent new funds. This recommendation was endorsed by the Provost and, in March 2007, the Board of Regents authorized President Dynes to proceed with development of a multi-year funding plan to accomplish funding of the Final Report recommendations.

At that time the Board also re-affirmed that the University Registration Fee (one of two Universitywide fees that all enrolled students must pay) as the appropriate source to fund campus student mental health needs. Regents' policy provides that the Registration Fee is for support of campus services that are complementary to, but not a part of, the instructional program, including specifically services relating "to the physical and psychological health and well-being of students." Finally, the Board approved a dedicated 3% increase to the Registration Fee for 2007-08 for campus student mental health needs, which will generate approximately $4.6 million in permanent new revenue for campuses to begin implementation of the Final Report recommendations. The University recognizes that this is only a first-step towards the approximately 25% increase to the Registration Fee that will ultimately be required to meet the campus needs identified by the Vice Chancellors for Student Affairs in their initial recommendation to the Provost. The Campus Security Task Force recognizes that implementation of the Student Mental Health Committee recommendations has already begun, and will continue to progress in stages, as funding becomes available.

Funding of Communications and Campus Safety

Unlike the current commitment of The Regents to proceed with a multi-year funding plan addressing the recommendations of the Student Health Committee's Final Report, the funding for implementation of the other recommendations of the Campus Security Task Force related to communications, preparedness, response, and mitigation has not yet been definitively identified or allocated. However, several potential funding opportunities are being evaluated.

UCOP Risk Services will fund the security surveys for existing campus buildings as part of the University's ongoing insurance program. The University's insurance coverage will also fund security surveys within the context of design review for new University construction.

Although UCOP Risk Services will fund the security surveys, remediation costs will be borne by the campuses. However, it is worth noting that the Office of Risk Services has established a systemwide loss prevention and control program – 'Be Smart About Safety' (BSAS) [http://www.ucop.edu/riskmgt/bsas/welcome.html].

Each year, Risk Services budgets a portion of its total allocation to fund proactive projects at the campus and medical centers. This funding is intended specifically to reduce the frequency and/or severity of potential losses and accidents.

Under the BSAS program, campuses may submit proposals to Risk Services for review and approval. Many of the specific campus recommendations of the Task Force might be funded with current funds already provided to the campuses under the program or with advance funding dollars delivered against probable future BSAS funding.

Some funding opportunities may exist through state or federal programs. For example, public safety radio communications interoperability qualifies for funding under the federal Homeland Security program, but the University has continually been severely underfunded from the highly competitive and limited 'state agency' pool of homeland security funds. The University will continue to pursue cost-effective state and federal funding, however.

In addition to the internal University funding options currently being evaluated, the University should identify and pursue external funding to address all of the Task Force recommendations through a combination of state, federal, and other fund sources.

Implementation

Regents' Standing Order 100.6, "Duties of the Chancellors," provides that "the Chancellor shall be responsible for the organization and operation of the campus, its internal administration, and its discipline." This responsibility extends to the safety and security of his or her campus. Each Chancellor shall report periodically to the President (in a way and according to a schedule to be subsequently determined by the President and communicated to Chancellors following final issuance of this Report) on progress towards further improving the safety and security of his or her campus, including progress towards implementation of the recommendations contained within this Report.

Summary

While no campus can be immune from the threats of violence that exist in larger society, the University should do everything feasible to create safe and secure campuses. Each of the three Workgroups recognized that each University campus is, in effect, a small city and that each of the campuses has differing circumstances and needs. The Chancellor of each campus is responsible for the public safety of the campus and must be enabled to fulfill that function as appropriate for the campus. This basic principle informed the recommendations of each Workgroup whenever possible.

The reports of the three Workgroups and their respective specific recommendations have been endorsed by all members of the Task Force and taken together constitute the recommendations of the full Task Force. Combined, the three Workgroup reports form the heart of the UC Campus Security Task Force Report.

The recommendations of the Task Force should serve as a starting point for each campus to review, develop and enhance its current policies, practices, programs, systems, and protocols in the manner that best fits the particular campus.

Report of the Student Mental Health Workgroup

Workgroup Members

Joel Dimsdale, Professor of Psychiatry, UCSD (Co-chair)
Michael Young, Vice Chancellor—Student Affairs, UCSB (Co-chair)
Ben Allen, 2007-08 Student Regent, UCB
David Birnbaum, University Counsel, UCOP
Greg Cendana, student representative, UCLA
Paul Henisey, Chief of Police, UCI
Janina Montero, Vice Chancellor—Student Affairs, UCLA
John Oakley, 2006-07 Chair, Universitywide Academic Senate, UCOP
Judy Sakaki, Vice President—Student Affairs, UCOP

Clint Haden, Director—Campus Life, Student Affairs, UCOP (staff to the workgroup)
Valery Oehler, Associate Director—Campus Life, Student Affairs, UCOP (staff to the workgroup)

Introduction

In the University's continuing efforts to help ensure the safety and security of its students, faculty, staff and visitors, the specific circumstances of the Virginia Tech shootings have reinforced the importance of having in place comprehensive, robust, and well-funded campus student mental health services and associated prevention, intervention, and education programs. These preventative services and programs are the University's first and best line of defense in materially reducing, if not altogether eliminating, the possibility of such a catastrophically violent series of events also occurring on a University of California campus at some point in the future.

Workgroup Charge

The charge to the Student Mental Health Workgroup was to examine—from the perspective of the University's campus student mental health services and associated prevention, intervention, and education programs—the University's preparedness for responding to and (more importantly from the perspective of the Workgroup, *preventing)* the occurrence of an event akin to the April 16, 2007 shootings at Virginia Tech.

Scope of Work

The Workgroup identified the following three areas for review:

> I. The current state of readiness of the University's campus student mental health services and associated prevention, intervention, and education programs, and its future plans for improving those services and programs;

II.   Potential changes to State and federal law and/or University policy to increase campus security with respect to the threat of student mental health-related incidents; and

III.   The current effectiveness of the University's communication and information-sharing mechanisms in the area of student mental health, with specific recommendations for the future improvement of these mechanisms.

I.   Current State of Readiness of Campus Student Mental Health Services and Associated Programs

Background Review and Analysis

The Workgroup reviewed the University's recent progress in its ongoing self-assessment of its student mental health needs, highlights of which are as follows:

Nearly eight months *before* the Virginia Tech shootings at Virginia Tech, on September 20, 2006, the Final Report of the University of California Student Mental Health Committee (See Appendix C) was presented to the University's Board of Regents.

In response to the growing realization that the nature and magnitude of student mental health services needs was changing both nationally and at the University of California, and that the University was struggling to keep pace, the Student Mental Health Committee was created by University President Robert C. Dynes and Provost Wyatt R. Hume in December 2005 to "study student mental health issues within the University". The Committee's findings strongly confirmed that initial realization, portraying a "stark new reality" of student mental health-related needs that had grown dramatically both in frequency and severity in recent years that were putting significant stress on the University's services and programs in this area. Finally, the Report findings called for "aggressive intervention" on the part of the University that "must include a systematic review of policy, enhanced communication mechanisms, and a renewed commitment to campus-wide collaboration along with an infusion of new resources commensurate with both the nature and magnitude of the challenge now facing the University."

In the Recommendations section of the Committee's Report, a comprehensive three-tiered "Plan of Action for Creating Healthier Campus Learning Communities" was outlined that progressively moved from the immediate staffing and programmatic needs of campus student mental health services (Tier I), to a broader program of targeted interventions for particularly vulnerable student groups and the strengthening of staffing levels in key campus student support services (Tier II), and finally on to a broad base of preventative efforts engaging the entire campus community (Tier III). Subsequent consideration by UC campuses of the proposed Plan of Action resulted in the development of a series of Provisional Campus Blueprints for Implementation of the Student Mental Health Report Recommendations (see Appendix D). These Blueprints reveal a remarkable consistency in the service needs from campus to campus, with a final price-tag for implementation of all of Tier I, most of Tier II, and some of Tier III totaling approximately $41.5 million in permanent new funding across the system.

Recognizing the importance of the need, the Board of Regents expressed its strong support of the Report in its entirety and at a subsequent meeting (March 2007) charged the President with developing a multi-year plan to fund in full the Report recommendations. As a first step in that multi-year plan, which is currently under development by the University's Office of the President, The Regents also approved a 3% increase to the University Registration Fee (a fee paid by all students for support of student services that are complementary to the core academic functions of the University and that improve the quality of student life) for 2007-08 for support of campus student mental health needs. This increase will generate an additional approximately $4.6 million in permanent funding which is a beginning towards achieving the total $41.5 million first-phase cost.

To help ensure that the Report recommendations are actualized in a timely and fully responsive way, the Provost of the University has also recently created a Student Mental Health Oversight Committee to monitor progress both in securing the needed funding and in ensuring that the Report recommendations are implemented once that funding has been secured. The present Student Mental Health Workgroup of the UC Campus Security Task Force is closely linked with the work and membership of that Oversight Committee, sharing the same co-chairs and partially overlapping agendas.

Apart from its efforts to secure adequate internal permanent funding, the University is also simultaneously pursuing extramural funding opportunities to provide complementary and enrichment support for its core student mental health programmatic and services needs. For example, the State Mental Health Services Act Oversight and Accountability Commission recently adopted a Student Mental Health Initiative that will make available $34 million in grants (for a share of which the University intends to compete) on a matching-fund basis to the public higher education segments in California for support of student mental health training, peer-to-peer support, and suicide prevention programs.

The Student Mental Health Workgroup's examination of the University's progress to date in assessing its student mental health-related needs was informed by the Workgroup's strong conviction that the provision of a broad array of student support services and student life opportunities is critical to creating healthier campus communities.

The Workgroup also believes that a well-funded, robust, comprehensive, and interconnected network of student-mental-health related services is the first and best line of defense in facilitating the early identification and treatment of students presenting mental-health-related behavioral issues. These front-line services can be complemented by the ready availability of an appropriately responsive array of other campus prevention, intervention, and educational programs. Acting together, these programs and services will provide the strongest realistically achievable insurance available to the University for *preventing* the occurrence here of a Virginia-Tech-like tragedy.

Recommendation

- The University should fund the recommendations of the Student Mental Health Committee Final Report (See Appendix C) in their entirety, as specifically articulated in the associated Provisional Campus Blueprints for Implementation of the Report Recommendations (See Appendix D).

II. Potential Changes to Law and University Policy: Balancing Individual Rights with Public Safety

Background Review and Analysis

The federally commissioned Report to the President on Issues Raised by the Virginia Tech Tragedy (See Appendix B) issued by the U.S. Department of Health and Human Services on June 13, 2007 highlighted the range of obstacles campus administrators face in navigating the maze of federal and state privacy laws in their efforts to share information with colleagues about students exhibiting severe psychological behaviors. In some instances, the problem may originate with the law itself, and can be addressed only if the fine line between protecting the individual's right to privacy and the institutional need to share information can be re-drawn. In other instances, the problem is rather one of misperception on the part of campus administrators of what the law legitimately allows, and can be addressed through better information-sharing protocols and training on the part of the institution. Finally, apart from considerations of student privacy, there are also institutional policies relating to student behaviors (other than those that may be strictly required under the law) that may merit re-examination. The Student Mental Health Workgroup examined specific proposals relating to each of the above three considerations.

Re-drawing the Line on Privacy Law

First, the Workgroup examined a preliminary proposal that was developed by the University's Office of the General Counsel in response to "continuity of care" concerns that have been raised by University of California campuses with respect to students who have been involuntarily admitted to psychiatric hospitals for observation under so-called "5150" 72-hour involuntary holds because their behaviors posed a significant immediate risk either to themselves or others. Under current federal law (the Health Insurance Portability and Accountability Act) information regarding the timing of release of such patients is protected as a matter of patient privacy and cannot be released by the holding hospital to others unless state law specifically provides otherwise. The proposal considered by the Workgroup would amend the California Welfare and Institutions Code to require such disclosure by hospitals to college and university administrators with responsibility for campus student housing, when the held student is resident in such housing, and when the hospital is specifically requested by the college or University to disclose information about the timing of the student's release. Having this information would ensure that the college or university would be alerted to the return of that student to institutional housing to try to ensure the provision of continuity of care. Following extensive discussion of the proposal by the Workgroup, based on preliminary comments received from campus counseling and psychological services, campus student housing offices, and student health services that reflected

a wide range of perspectives within the University of California system, the Workgroup concluded that the proposal was of sufficient merit to warrant a broader and more thorough review over the coming months, with expanded opportunities for input by the entire University community including faculty, staff and students.

Proposed Changes to Internal University Policy

In addition, the Workgroup examined the preliminary draft of a proposed Policy on Involuntary Psychiatric Withdrawals, which was also developed by the University's Office of the General Counsel. The draft originated from the perceived campus need for an instrument to allow for the involuntary withdrawal from the campus community of a student exhibiting threatening psychological behaviors to the degree that there is reason to believe that the student poses a significant risk to him/herself or others, threatens or endangers University property, or disrupts the stability and continuance of normal University operations and functions. Again, following extensive discussion of the preliminary draft policy by the Workgroup, as informed by preliminary comments received from a variety of campus administrative units reflecting a wide range of perspectives both pro and con, the Workgroup determined that the proposal was of sufficient interest to warrant a broader and more thorough review, with expanded opportunities for input by the entire University community, including faculty, staff and students.

The Workgroup's consideration of the above two proposals was everywhere informed by the fact that it recognizes and respects the delicate balance that exists under current law and in University policy between individual privacy and other individual rights and communal needs. Nonetheless, the Workgroup believes that, in the wake of traumatic societal events like the Virginia Tech shootings, any thoughtfully considered proposed adjustment to that balance merits, at a minimum, serious discussion by the broader University community. Therefore, while the Workgroup did not expressly recommend either the adoption or the rejection of either proposal discussed above, given the complexity of the issues raised, the Workgroup strongly believes that such a broader University review of these proposals should in fact take place over the coming months.

FERPA

Finally, the Workgroup examined criticisms of the federal Family Educational Rights and Privacy Act (FERPA) that have been widely reported in the media which allege that the provisions of FERPA are an impediment to the appropriate sharing of student-mental-health-related information among University officials, concerned family members, and designated others. These allegations do not appear to be supported by a close reading of the law itself, which the University's Office of the General Counsel has reviewed and concluded provides adequately for the sharing of student information among campus officials and others as appropriate where there are legitimate campus safety concerns, despite the widespread misperception among college and university officials nationwide that such is not in fact the case. This misperception is readily addressed through stepped-up training and education programs on the part of the institution. In addition, several provisions in the University's own policies regulating the disclosure of information about students are more restrictive than what is required under federal law. State law requirements may be more restrictive. The University should re-

examine these provisions, in consultation with the General Counsel's office, in light of the heightened awareness about campus safety concerns coming out of the Virginia Tech shootings. The University of California's need for strengthening its training and education programs to ensure that its officials have an adequate and accurate understanding of FERPA and related privacy laws with respect to the permitted disclosure of student information in specified circumstances is addressed in Section III (Current Effectiveness of the University's Student-Mental-Health-Related Communication and Information-Sharing Mechanisms) of the Workgroup Report, below.

Recommendation

- The Office of the President, working closely with the campuses, should continue its examination of prospective changes to student and patient privacy and related laws, as well as to the University's own internal policies and protocols. As part of this examination, the Office of the President should coordinate a broad-based campus review process of specific proposals immediately on issuance of the Task Force's Final Report, to ensure that any final recommendations or actions of the University will take into full consideration the views of all segments of the University community.

III. Current Effectiveness of the University's Student-Mental-Health-Related Communication and Information-Sharing Mechanisms

Background Review and Analysis

The federally commissioned Report to the President on Issues Raised by the Virginia Tech Tragedy (See Appendix B) also addresses issues of misperception regarding permitted communications on the part of college and university officials even when the law allows for the sharing of otherwise protected information on health and safety grounds. In the course of its review, the Workgroup identified similar obstacles in place at the University of California, despite the existence of campus multidisciplinary behavioral management teams and associated highly developed crisis management/response protocols to help ensure that accurate, efficient, and rapid communication occurs across campus units during a crisis, as well as to help provide for the maintenance of student and campus safety. The Workgroup found that on-the-ground practical difficulties relating to the communication of sensitive information about students are commonly exacerbated by the inherent complexities of interconnected State and federal privacy laws, differing legal constraints on the sharing of information depending on the specific functional roles of particular campus administrators, and the inevitable attrition of staff over time which mandates continued efforts at training to ensure that all staff are kept current on the institution's communication protocols.

In connection with its broader review of this area, the Workgroup also noted the existence at all campuses of a wide variety of successful, pro-active student-mental-health-related prevention, intervention, and education programs, including (with some variation campus to campus) informational presentations and training workshops to assist staff, faculty, and other students in identifying students who manifest mental-health-related behavioral issues and who may thus be at risk for harming either themselves or others; web-based and printed informational materials to

help at-risk students understand that help is near at hand, and to assist others in how to respond to such students; suicide prevention hot-lines; and a broad range of public programs tied into a periodic campus awareness day or week.

Recommendations

- Each campus should have in place one or more coordinated multidisciplinary behavioral management teams, and provide for regular and recurring reviews of the structure, make-up, and related protocols of its team or teams with special reference to the scope, adequacy, accuracy, and effectiveness of the communication and information-sharing mechanisms that connect the team(s) to the campus and the campus to the team(s).

To assist campuses in these tasks:

- the University's Office of the General Counsel should continue to maintain among its legal staff an attorney specifically trained in the area of mental health-related law to serve as a student mental health specialist to campuses, who can then coordinate discussion among, and provide legal clarifications to, all campus staff whose functional areas (e.g., counseling and psychological services, campus police, other legal counsel, campus housing officers, deans of students, etc.) are impacted by students exhibiting psychologically disturbed behaviors;

- the Office of the General Counsel should also prepare and make available concise written systemwide legal guidelines and other reference materials that delineate how, with whom, and for what purposes information regarding psychologically disturbed students can be shared; and

- the Office of the President, working with the Office of the General Counsel, should initiate the development of regular information-sharing and communications training programs that involve key campus partners (counseling and psychological services, campus police, other legal counsel, housing officers, deans of students, etc.), and these programs should be informed by a common set of systemwide disclosure standards and communications protocols to be developed under the coordination of the Office of the President in close consultation with the campuses and with the Office of the General Counsel.

Appendices to Student Mental Health Workgroup Report

UC Student Mental Health Committee Final Report (See Appendix C)
Systemwide Summary: Provisional Campus Blueprints for Implementation of the Student Mental Health Report Recommendations (See Appendix D)

Report of the Crisis Communication and Emergency Preparedness Workgroup

Workgroup Members

Kristine Hafner (Co-Chair), Associate Vice President - IR&C, UCOP
Bob Charbonneau (Co-Chair), Emergency Manager, UCOP
Linda Bisson, Professor and Division Chair, Academic Senate, UCD
Joel Dimsdale, M.D., Professor of Psychiatry, UCSD
Vicky Harrison, Associate Vice Chancellor and Chief of Police, UCB
Valerie Lucus, Emergency Manager, UCD
Tom Vani, Vice Chancellor—Business and Administrative Services, UCSC

Introduction

The safety and security of students, faculty, staff, and visitors on all UC campuses is the highest priority for the University of California system. In addition to having effective plans to respond to extraordinary and disastrous events, campuses have a responsibility to notify and inform the campus community of dangerous or potentially dangerous situations and incidents, and should provide timely and specific directions so the campus community can make informed decisions and exercise good judgment and common sense to ensure their own personal safety. The Crisis Communication and Emergency Preparedness Workgroup of the University of California Campus Security Task Force examined a range of issues related to UC emergency response capabilities.

Workgroup Charge

The charge of the Crisis Communication and Emergency Preparedness Workgroup was to review current campus crisis communication and mass notification capabilities, plans, policies, and procedures, recommend minimum capabilities, benchmarks, and best practices, and identify any gaps between these areas. While the immediate effort is directed at issues surrounding an 'active shooter' scenario, the intent of this workgroup is to expand this review to an "all-hazards" perspective once this initial work is complete. Therefore, this workgroup will focus initially on our overall readiness to respond, and will expand to the broader scope of ensuring resources, plans, and policies are in place for future incidents.

Scope of Work

The Workgroup identified the following nine areas for review:

- In conjunction with the Campus Safety workgroup, describe and agree upon the plans, processes, and procedures that need to be in place to support effective crisis communication and rapid campus-wide emergency notifications.

- In conjunction with the Campus Safety workgroup, clarify roles, responsibilities and accountability for activating, formulating, and disseminating timely campus-wide emergency notifications.
- Document the current state of campus-wide emergency notification systems and capabilities at all UC campuses.
- Identify and evaluate available emergency notification system approaches and technology options, and make recommendations on which ones to pursue.
- Address resources required to implement basic and advanced technical solutions, including the source of funds for efforts that go beyond current campus capabilities.
- Address campus-wide emergency contact information data management challenges, options, and recommendations to efficiently maintain an accurate inventory.
- Define minimum baseline capabilities, benchmarks, lessons learned, and best practices as well as analyzing the gap between these and the current efforts.
- Identify opportunities for systemwide collaboration and leveraging resources.
- Provide general campus emergency preparedness recommendations as appropriate.

Consistent with the defined scope of work, the Workgroup established the following guiding principles:

- Emergency notification systems should be both layered and redundant – *no single means of communication should be solely relied upon to reach the entire campus community.*

- A set of minimum capabilities for emergency notification and crisis communication should be implemented at each campus – *each campus should establish and maintain plans, procedures, and emergency notification systems that meet a standard baseline.*

- There should be a robust underlying infrastructure to support, maintain, and test the systems – *adequate resources should be provided to accomplish these objectives.*

- Effective communication requires a comprehensive Crisis Communication Plan – *each campus should develop an interdisciplinary team and plan that supports timely warning and notification, emergency public information, and media management during a crisis or critical incident.*

I. Crisis Communication

Background Review and Analysis

The goal of crisis communication is to proactively convey urgent, necessary, and desired messages in an effective and organized manner to both the entire campus community and external audiences including the general public and media. Campuses face a wide array of potential crises stemming from incidents ranging from mass shootings to natural disasters. In 2005, the systemwide Safety, Security and Anti-Terrorism (SSAT) Committee facilitated comprehensive Hazard Vulnerability Assessments at every campus. These assessments identified and evaluated physical threats facing the University, including natural hazards, human-

caused events, technological hazards, and terrorist acts. Campus crisis communication should consider campus-specific risks and threats that were evaluated during this process.

Recommendations

- Each campus should develop a Crisis Communication Plan that clearly defines roles and responsibilities as well as delegations and lines of authority for various campus officials in order to avoid delays, inconsistencies, and confusion in the process of issuing alerts and warnings during an emergency situation or critical incident.

  Preliminary guidelines for campus Crisis Communication Plans are included in Appendix E. Note that systemwide public information and emergency management personnel are still working to develop additional campus guidance documents.

Warnings are effective only if they are accurate and result in appropriate action. Effective warning messages should:
- Be brief (preferably less than one minute)
- Present discrete ideas in a bulletined fashion
- Use non-technical language
- Use appropriate text/graphics geared for the campus community
- Provide official basis for the hazardous event message (UCPD reports…)
- Provide most important information first, including any standardized headlines
- Describe the areas affected and time (if events are moving)
- Provide level of uncertainty (if applicable)
- Provide a brief action-oriented statement for appropriate campus-wide response (accurate and specific instructions or directives)
- Describe where more detailed information can be found

The annual University emergency management status report is based upon the National Fire Protection Association (NFPA 1600) National Standard on Emergency/Disaster Management and Business Continuity Programs. The University has voluntarily adopted this standard which recommends the following minimum elements for crisis communication and emergency public information:

Crisis Communication and Public Information
- *Establish procedures to disseminate and respond to requests for info (both internal and external including the media)*
- *Establish and maintain disaster/emergency public information capability including media contact facility; system for gathering, monitoring, and disseminating emergency information; method to coordinate and clear information for release; pre-scripted information bulletins; special needs populations; and protective action guidelines/recommendations (evacuation or shelter-in-place)*
- *Implement public awareness program for identified hazards and procedures to advise the public of threats to people, property, and the environment*

II. Emergency Mass Notification Systems

Background Review and Analysis

The University currently has some type of mass notification system in place at every campus and medical center. Most commonly, these include broadcast email and voicemail messages to campus accounts/phones, webpage banners or links, emergency hotlines or call-in numbers, and mobile public address systems in public safety vehicles. Medical centers also have overhead building public address systems in their hospital facilities, and text pagers. Appendix F contains a summary of the types of mass notification systems currently in place as reported by the campuses and medical centers.

Recommendations

- Each campus should complete a 'Gap Analysis' which inventories and evaluates its current emergency communications practices, capabilities, and needs with the objective of identifying and closing any gaps.

The gap analysis of communications systems should ideally occur within the context of a more comprehensive analysis of campus-wide emergency management and response capabilities. Appendix G contains an example of an excerpted emergency communications gap analysis conducted as part of a comprehensive campus-wide assessment.

- Each campus should select appropriate systems based on the following criteria. An effective emergency mass notification system should:

    o Be reasonably easy to set up, maintain, and manage
    o Be continuously available and reliable
    o Operate within the capacity limitations of any transmitting systems
    o Possess redundant communications capabilities
    o Be built to handle a campus worst-case scenario
    o Effectively deliver messages that are time-sensitive, clear, easily understandable, and specifically direct the actions of the recipients
    o Effectively alert as many people on campus as quickly as possible
    o Account for visually/hearing impaired persons and those for whom English is second language
    o Ensure that off-campus responders are aware of the notification system

- Selected systems should include the following basic methods of emergency mass notification (See Appendices H and I for a further description of these technologies and their relative benefits.)

    o Mass email distributions and mass voicemail broadcasts
    o Automated message calling systems (Reverse 911)
    o Mobile or stationary electronic message screens/signs
    o Web-based messages (web pages, banners, pop-ups, etc.)

o Mobile public address systems (hand carried or vehicle-based)
o Stationary public address systems (sirens)
o Building overhead public address systems
o Text-messaging to cellular phones or pagers
o Radio/television stations, including Emergency Alert System (EAS) messaging
o Closed circuit television (CCTV) systems

The annual University emergency management status report is based upon the National Fire Protection Association (NFPA) 1600 National Standard on Emergency/Disaster Management and Business Continuity Programs. The University has voluntarily adopted this standard which recommends the following minimum elements related to emergency communications and warning systems:

<u>Communications and Warning Systems</u>

- *Establish, regularly test and exercise communications systems/procedures*
- *Develop and maintain notification/alerting capability for response personnel*
- *Develop and periodically test campus-wide emergency alerting system and protocols/procedures/processes*
- *Address communications needs/capabilities to support response/recovery plans*
- *Address inter-operability of multiple emergency response agencies*

The Florida Gubernatorial Task Force on University Campus Security report (See Appendix B) also emphasizes the importance of taking specific measures to inform the campus community upon addition of any notification systems or devices, to provide notification procedures to all emergency responders (on/off campus), and to develop standards for notification systems and devices and promulgate a "best practices" guide for use, maintenance, and frequency of system testing.

III. Information and Data Management

Background Review and Analysis

Effective deployment and implementation of any emergency mass notification system depends on effective and efficient management of campus-wide contact information.

Recommendations

- Each campus should identify policies and options for obtaining accurate and current contact information for students, staff and faculty. Locations should design solutions that facilitate the input of data from existing campus-wide directory information or and/or HR database applications to ensure that an accurate repository of contact information for the entire campus community is constantly maintained. Strong consideration should be given to solutions that require both:

o faculty and staff to update emergency contact information during the annual benefits enrollment period; and
o students to update emergency contact information while registering for classes.

- Campuses should take appropriate information security measures to prevent unauthorized access to or use of the contact information consistent with existing University policy and guidelines for information security as expressed in Business and Finance Bulletin IS-3, Electronic Information Security: http://www.ucop.edu/ucophome/policies/bfb/is3.pdf.

IV. Emergency Preparedness

Background Review and Analysis

The National Preparedness Standard on Disaster/Emergency Management and Business Continuity Programs (National Fire Protection Association, 2004) forms the basis for the annual system-wide status report on campus emergency management programs. This collaboratively developed standard has been universally endorsed by the American National Standards Institute (ANSI), the 9-11 Commission, US Congress, and the federal Department of Homeland Security.

Recommendations

- Each campus should work towards full emergency management program implementation based on the NFPA National Standard. Major program elements include:
  o Designate an emergency manager at each campus
  o Establish a program advisory and review committee/council
  o Periodically conduct a Hazard Vulnerability Assessment
  o Establish resource and logistical management capability
  o Develop various program plans including emergency operations, prevention/ mitigation, recovery, and continuity plans
  o Use the Incident Command System to manage major incidents
  o Establish and test campus-wide notification and alerting systems
  o Develop standard operating procedures to support program/plans
  o Establish primary and alternate Emergency Operations Centers
  o Implement campus-wide training and education programs
  o Annually conduct exercises, evaluations, and corrective actions
  o Establish crisis communication and public information capability

V. Systemwide Opportunities and Recommendations

Background Review and Analysis

The ten-campus University system has a wealth of resources and expertise spread across the entire state. Whenever possible, the University should leverage its significant systemwide resources and purchasing power, and identify, capture, retain, and transfer valuable knowledge and expertise to build on successes and lessons learned. By emphasizing collaboration, the

University can better develop and support strategic systemwide initiatives and planning efforts, and leverage economies of scale.

Recommendations

- Share best practices. Establish a systemwide multi-disciplinary forum that would share best practices in the areas of emergency preparedness, crisis communication, and emergency notification. This could include review of 'After-Action' reports and lessons learned, as well as technological solutions. This forum would review sentinel events that occurred on campuses with a view towards defining and implementing best practices.

- Leverage the systemwide IT contracting and strategic sourcing initiative for purchasing/licensing of resources and services in the areas of emergency preparedness, crisis communication, and emergency notification. An example is contracting with one or several vendors for Universitywide emergency notification systems.

- Leverage the current IT Disaster Recovery process to provide redundancy and back-up services between campuses.

- Provide additional funding to enhance existing emergency mass notification systems (e.g. - overhead paging or public address systems, text messaging capabilities, enhanced and reverse 911, etc.)

- Review systemwide building construction and remodel standards to incorporate best practice standards as it relates to emergency warning and notification systems.

- Specify funds/funding levels for each campus for emergency preparedness, response, management and recovery programs.

- Establish an emergency management council at each campus including administration executives, faculty, students and staff representatives to periodically review plans and activities similar to campus audit committees.

Appendices to the Crisis Communication and Emergency Preparedness Workgroup Report

Preliminary Guidelines for Campus Crisis Communication Plans (See Appendix E)
Summary of Campus Mass Notification Systems (See Appendix F)
Emergency Communications Gap Analysis – Campus Example (See Appendix G)
Overview of Mass Notification System Technology Solutions (See Appendix H)
Pros and Cons of Selected Mass Notification Systems (See Appendix I)

Report of the Campus Safety Workgroup

Workgroup Members

Karl Ross (Chair), Chief of Police and Chair of Council of UC Chiefs, UCLA
Mary Croughan, Professor of Obstetrics, Gynecology, and Reproductive Sciences, UCSF
Victoria Harrison, Chief of Police, UCB
Paul Henisey, Chief of Police, UCI
Janina Montero, Vice Chancellor - Student Affairs, UCLA
Tom Vani, Vice Chancellor - Business and Administrative Services - UCSC
Michael Young, Vice Chancellor - Student Affairs, UCSB

Gail Riley, Legislative Director and Police Services Coordinator - Business Operations, UCOP
(staff to the workgroup)

Introduction

The safety and security of students, faculty, staff and visitors on all UC campuses is of the highest priority for the University of California system. While all UC Police and Emergency Services Departments have the personnel, policies, resources, equipment, training and support to respond to a wide range of critical incidents, including such an event as the devastating active shooter incident at Virginia Tech, it is important to review and re-evaluate our capabilities. Each campus should have a comprehensive and integrated public safety system and strategy with clear roles and responsibilities in order to provide the best possible response to these events.

Workgroup Charge

> The charge of the Campus Safety Subcommittee Workgroup is to review current campus practices, procedures and capabilities of the law enforcement and emergency response departments in the UC system. While the immediate effort is directed at issues surrounding an 'active shooter' scenario, the intent of this workgroup is to include an analysis of the ability to respond to all violent critical incidents. The definition of a violent critical incident certainly includes an active shooter, but it could include any act of violence from a viable bomb threat to a criminal homicide or an act of terrorism. We recognize that it is not sufficient to be able to just respond to incidents of violence but we must look for ways to improve our abilities to prevent such acts of violence from occurring on our university campuses.

Scope of Work

The Workgroup identified the following six areas for review:

1. Assess the capability of interoperability communications for emergency first responder personnel.

2. Examine personnel staffing and equipment necessary to adequately respond to violent critical incidents.

3. Review the level and standards of training for emergency first responder personnel and other campus community members.

4. Review the safety and security of the current system infrastructure and identify opportunities for improvement.

5. Review the role of a multi-disciplinary team to identify and address behavioral risks.

6. Identify and review applicable policies and procedures regarding critical incident management and response systemwide.

I. Behavioral Risk Assessment Capability

Background Review and Analysis

The ability to conduct behavioral risk assessments should exist on every campus and can serve as an effective means to address problems before they turn violent. The assessment should be conducted by a multi-disciplinary team involving appropriate campus representation. The purpose of this team is to meet on a regular basis to share information and formulate action plans on potential circumstances or individuals who pose a threat to the campus community. The team should include senior managers from key departments such as Student Affairs, Human Resources, Student and/or Faculty/Staff Counseling, Police Department, Dean of involved Academic School, Campus General Counsel, and others as necessary given the nature of the threat. The sharing of information in this manner is critical to effective decision-making and is authorized by law when an individual poses a threat to themselves or to others.

Recommendations

- Each campus should establish an interdisciplinary behavioral risk assessment team to address issues, problems or individuals who may pose a threat to the campus community. The team would be responsible for developing an action plan to address the threat.

- Each campus should communicate to its staff, faculty and students the purpose of the behavioral risk assessment team. Each campus should provide training to staff and faculty concerning the appropriate sharing of critical information with authorized campus managers, academic leaders, and staff representatives.

- A multi-disciplinary training seminar or conference should be convened for all UC campuses to share lessons learned, action plans, critiques and personal insights from incidents and events experienced across the system. The seminar should involve key management and administrative personnel to share and discuss best practices.

II. Campus Community Training

Background Review and Analysis

Training is an important component of any effective emergency response to critical incidents. While each campus Police Department currently meets all statewide mandated training standards, the level of training to our campus communities on what to do in the event of a violent critical incident is inconsistent. Training and information on how to respond to violent critical incidents should also be provided to staff, faculty and students.

Recommendations

- Each campus should develop training for staff, faculty and students on the recognition of warning signs of potential violent behavior and what actions to take when these warning signs are noted.

- Each campus should provide training to all members of the campus community on what actions to take if a violent critical incident occurs

- Training should be provided to the campus community on securing the campus procedures and evacuation procedures.

III. Emergency Communications

Background Review and Analysis

The events at Virginia Tech highlight the importance of communications in responding to a critical incident and coordinating resources to resolve such an emergency. Although the Emergency Preparedness and Communications workgroup has reviewed this area, this workgroup wanted to stress the vital importance of emergency communications interoperability by including this component in this report.

Communications in emergency circumstances is a critical part of an effective response by emergency service providers. Communications should be rapid, clear and effective between responding units, dispatch centers, emergency operations managers and campus administrators. A coordinated response of life saving services is essential to minimize the impact of violent critical incidents. Campuses need to assess the staffing level of police officers and other emergency personnel in order to respond fully to a violent critical incident such as an active shooter. In addition, our campuses will have to depend upon critical mutual aid resources including police officers, fire fighters and emergency medical service personnel from surrounding agencies.

The ability to communicate immediately and directly with all first responders is critical. UC Police Officers and other emergency personnel responding to an active shooter or other violent crime in progress must be able to inform outside responding units of the type and location of the incident, suspect description, weapons involvement, direction of travel, staging areas and

routing, along with other critical information. Any delays or miscommunication as the information travels through various channels and dispatch centers may hinder the rapid response of emergency personnel.

Public safety agencies should have the necessary equipment to communicate effectively in a wide range of violent critical incidents. Each campus should determine what the appropriate level should be for its campus community. One area where the UC system has not received sufficient support is from Department of Homeland Security funding. These funds have been provided through the Urban Area Security Initiative (UASI) which has been distributed to major urban areas. Most UC campuses are in these regions but have been largely excluded from obtaining funds to improve their security or ability to respond to a violent critical incident while many city and county agencies have received literally millions of dollars in grant funding. UC campuses have been identified as potential targets for terrorism and, in fact, are home to some of the highest attended sporting events, art and cultural exhibits, and controversial events while consisting of a target population in which an attack would have an overwhelming societal impact. It is important for the Office of the President, in conjunction with the UC campuses, to ensure that the campuses receive funding sufficient to address the most critical public safety needs.

Recommendations

- Each campus should assess its capability in receiving, processing and acting upon all emergency phone calls including 9-1-1 calls and Enhanced Wireless 9-1-1 (cellular 9-1-1) calls. The assessment should include a review of current dispatch operations and technologies to ensure the rapid access to critical information.

- Each campus should have communications interoperability with its immediate mutual aid and emergency services providers. Such capacity should include the ability to communicate directly with police, fire and emergency medical services including those from surrounding agencies while responding to and handling a critical event. The University should seek adequate funding to address this need. Communications interoperability should be tested or used on a regular basis.

- Each campus should assess the vertical integration of campus wide emergency communications. This assessment should include an analysis of technology improvements in information flow and should provide for the ability to produce and distribute an emergency communication to the campus community in a timely manner.

IV. Personnel and Equipment Resources

Background Review and Analysis

The number of personnel and the availability of equipment to respond to violent critical incidents are important keys to resolving these incidents in as quick and safe manner as possible. While it is neither possible nor appropriate to staff for the rare critical incident, it is necessary to provide an adequate staffing level to meet the on-going demands of large and active campus

communities. Each campus should ensure police officer staffing includes a sufficient number of officers to handle the routine calls for service, conduct proactive crime prevention patrols, and respond to emergency calls with as short a response time as possible.

Experienced and well-trained officers are the most important asset to any police department. Our campus police departments are no different. In this highly competitive and demanding job market for good police officers, the ability to recruit and retain our officers has become increasingly difficult, especially for many of our departments. Campuses must ensure they can attract and retain the most competent and experienced officers.

Likewise, public safety agencies must have the necessary equipment to respond effectively to a wide range of violent critical incidents. Each campus should determine the appropriate level of necessary equipment for its campus community.

Recommendations

- Each campus should assess their levels of staffing of police officers, emergency services providers and support staff to ensure an appropriate response to violent critical incidents.

- In addition, each campus should inventory their safety and emergency response equipment to ensure it is sufficient to address an active shooter or other violent critical incident.

- Each campus should conduct active shooter response training as part of emergency management exercises. The training should include mutual aid response agencies and training in the use of any specialized equipment.

V. Facilities and Infrastructure

Background Review and Analysis

Several Virginia Tech reviews address the difficulties in "locking down" a campus. UC campuses cannot be secured instantaneously in an emergency. Law-enforcement experts nationwide agree that a "lockdown" is simply not feasible on campuses the size of a small city. Even if a "lockdown" were possible, the numerous and sometimes conflicting emergency access systems can be an obstacle to implementation of emergency protocols. However, it is feasible to secure or "harden" individual buildings and facilities and to develop common entry technologies, such as electronic card key access.

Just as there are earthquake and fire standards incorporated in the design and construction of new buildings or in the retrofit of existing buildings, security and crime prevention standards should be part of routine inspections of existing building and engineered into the design of new buildings. Crime prevention through environmental design should be included in the design and development of all campus buildings and infrastructure. Enhanced security measures and inclusion of improved safety technologies can reduce the likelihood of crime and serve to deter criminal acts.

Recommendations

- Security surveys should be conducted on existing campus buildings and should include security recommendations, as necessary, for further evaluation, selection, and prioritization by the campus.

- Design review for all new buildings should include recommendations to enhance the security of the building.

VI. Policies and Procedures

Background Review and Analysis

Effective and appropriate policies and procedures are an important part of establishing the direction, organization and operation of any formal entity. Each campus has its Administrative Policies and Procedures and each campus Police Department keeps and maintains a Department Manual. In addition, there is the Universitywide Police Policy and Procedures (Gold) Book which establishes policies and procedures in a number of areas for all UC Police Departments. Included in these policy manuals is a wide variety of information and procedures pertaining to the response to emergency critical incidents.

Recommendations

- Each campus should ensure they have in place procedures to address:

  - Active shooter response
  - Emergency communications
  - Evacuation of campus facilities
  - Hazardous material incidents
  - Hostage/barricaded suspect
  - Incident command system
  - Major incident notifications
  - Risk assessment and mitigation
  - Access controls
  - Shelter in place
  - Threat management
  - Timely warnings
  - Use of force

- The scope and content of these procedures should be reviewed by the appropriate campus personnel on an annual basis and modify or revise as necessary and appropriate.

Campus Security Task Force Appendices

Appendix A. President Dynes' Letter to the Regents and
Charge Letter to Members of the Task Force
Appendix B. Links to Selected Virginia Tech Reviews

Student Mental Health Committee Workgroup
Appendix C. Student Mental Health Committee Report
Appendix D. Systemwide Summary: Provisional Campus Blueprints for Implementation of the
Student Mental Health Report Recommendations

Crisis Communication & Emergency Preparedness Workgroup
Appendix E. Preliminary Guidelines for Campus Crisis Communication Plans
Appendix F. Summary of Campus Mass Notification Systems
Appendix G. Emergency Communications Gap Analysis – Campus Example
Appendix H. Overview of Mass Notification System Technology Solutions
Appendix I. Pros and Cons of Selected Mass Notification Systems

Appendix A. President Dynes' Letter to The Regents and Charge Letter to Members of the Task Force

UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO   SANTA BARBARA • SANTA CRUZ

OFFICE OF THE PRESIDENT

Robert C. Dynes
President

1111 Franklin Street
Oakland, California 94607-5200
Phone: (510) 987-9074
Fax: (510) 987-9086
http://www.ucop.edu

April 30, 2007

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

Along with the national grief that has followed in the wake of last week's tragic shootings at Virginia Tech University have come questions about what can be done to prevent such a rampage from ever happening on a University of California campus.

In the days immediately following the tragedy, UC convened its Police Chiefs, Vice Chancellors of Student Affairs, and other relevant University officials to explore campus security measures; student mental health practices and policies; notification capabilities; emergency preparedness; and related legal issues.

The enclosed overview shows that the University of California has many sound practices, policies and systems in place with respect to these issues. At the same time, however, it is clear there is room for substantial improvement.

Therefore, I am appointing a UC Campus Security Task Force to study how the University of California campuses can enhance their security, notification processes, mental health services, and general preparedness. The Task Force will be co-chaired by Provost Rory Hume and Executive Vice President Katherine Lapp, and will be composed of a broad-based group of University security, student affairs, legal and emergency preparedness experts, and I also enclose a list of members for your information.

I am asking the Task Force to devote substantial time in the next two months to addressing these critical issues and to make recommendations to the Chancellors and me. I recognize that considerable work has already been done in a number of these areas, including student mental health and emergency preparedness, so I ask that these be reviewed in light of what we have learned from the Virginia Tech experience. In addition, I am asking the group to explore additional legal or legislative remedies that could improve the balance between privacy and security protections, particularly with respect to the proper University notification of parents when mentally ill students threaten violence against themselves or others.

Appendix A. President Dynes' Letter to The Regents and Charge Letter to Members of the Task Force

The Regents of the University of California
April 30, 2007
Page 2

There can be no greater priority than the safety of the University of California's students, faculty, and staff. While UC can take pride in the many positive and pro-active steps we have taken over the last several years, the Virginia Tech tragedy underscores that more can always be done to make our campuses safer and more secure, as well as less vulnerable and more resilient in the aftermath of any extraordinary disruption. This Task Force will help ensure that the University of California, in meeting that goal, fulfills its teaching, research and public service mission to the people of California.

Sincerely,

Robert C. Dynes

Enclosures

cc: Chancellors

Appendix A. President Dynes' Letter to The Regents and Charge Letter to Members of the Task Force

UC CAMPUS SECURITY: A POST-VIRGINIA TECH ASSESSMENT

Mental health

The University of California has played a leadership role in focusing on student mental health issues, going back to the December 2005 establishment of a Student Mental Health Committee. In presenting its final report to Provost Hume in September 2006, the Committee noted that mental health trends visible nationally are negatively affecting all UC campuses. In particular, the Committee found that:

- Following national trends, UC students are presenting mental health issues with greater frequency and complexity. As a result, the workload among mental health and other professionals on our campuses is increasing, not only because they have to address directly the increasingly complex needs of greater numbers of individual students but because they have to assist in the campus community's collective response to these needs.

- Budget trends within the University (and in the surrounding local communities) limit the capacity of campuses to respond to mental health issues and are manifested in longer student wait-times, difficulty retaining staff, and decreased services and programs. Student fees devoted to relevant services have remained relatively flat while the demand for and cost of providing those services has increased. This applies to direct mental health services and to the indirect mental health services provided by allied programs in campus safety, disability services, student life, residential life, learning support, and academic units.

  In response, The Regents in March voted to enhance mental health services provided to students. Given the serious and urgent need for enhanced mental health services, the University will set aside 43 percent of the revenue generated by the 7-percent increase in the registration fee -- approximately $4.6 million -- to fund initial steps in a recommended $40 million multi-year plan to enhance mental health services.

- This increasing demand and declining capacity pose a threat to the learning environment because of their significant adverse impacts on faculty, staff, and students. The Committee urged the University to take action to ensure that its campuses can create healthier learning environments. A comprehensive response to these concerns was summarized in a plan of action delineated by the Committee in its Report. This plan envisions action on restoring critical mental health services; implementing and augmenting targeted interventions through education, support and prevention programs and restoring staffing levels in those units best poised to assist high-risk students; and taking a comprehensive institutional approach to creating healthier learning environments by enhancing the full spectrum of student life services, and revising administrative policies as well as academic practices that influence communication and collaboration around these issues.

Appendix A. President Dynes' Letter to The Regents and Charge Letter to Members of the Task Force

A full copy of the report can be found at
http://www.universityofcalifornia.edu/regents/regmeet/sept06/303attach.pdf

Campus Security

In the fall of 2003, the University of California established the systemwide Safety, Security and Anti-Terrorism (SSAT) Committee to study the state of the University with respect to overall security, exposure to threats, and ability to respond to emergencies such as an active shooter event as occurred at Virginia Tech. Other identified threats included catastrophic earthquakes, laboratory building fires, workplace violence, and animal or crop eco-terrorism, among others.

The result has been the development of the Hazard Vulnerability Assessment (HVA) initiative, which provides an overview of the campus risk assessment process, summarizes the systemwide hazard vulnerability assessment findings and makes recommendations for University-wide risk reduction and mitigation strategies.

The SSAT committee was aided in the review and development process by a nationally recognized consultant, James Lee Witt & Associates.

A potential shooting incident on a campus was ranked the seventh-highest systemwide threat, and is closely related to the threat of workplace violence. Seven campuses listed this threat in their "top 10" threat list. The Committee has noted that incidents of threatening or violent workplace behavior can happen anywhere on campus and at any time. Incidents may be triggered by disgruntled current or former students, staff, or faculty or a disturbed partner or spouse. In addition to aberrant behavior by a person related to the campus, violent incidents may also be carried out by individuals from outside the campus community targeting either the institution or a specific person on campus, or motivated by criminal intent such as robbery or theft.

In regard to a potential shooting incident, the campuses have protocols in place to prepare and guide campus police officers and dispatchers. These include specific live campus training for rapid response to shooter scenarios, joint training with adjacent jurisdictions, disaster response drills, and simulator training. In addition, all the campuses have specialized equipment to handle an active shooter on campus.

Because of the very nature of higher education, a lock-down of any of our campuses is difficult, if not impossible. However, all campuses have means to limit entrance and egress of the campuses and thus restrain the movement of an active shooter. Some, but not all, of the campuses can electronically lock-down specific campus buildings.

All campuses are required under state law to have memoranda of understanding with surrounding jurisdictions governing response and mutual aid and most have radio linkage with those jurisdictions to ensure a fully coordinated response in the event of an emergency.

Many campuses have also established multi-divisional operations composed of several campus units with special expertise and professional training, including police, to identify and address disruptive, intimidating, threatening or violent behavior of any members of the campus community.

In addition to University police resources, campuses also rely on campus-wide and specific building security and safety measures and systems, such as building access controls, surveillance systems, panic and alarm systems, cashier office security measures, and designs for high-risk office that incorporate multiple safety features and prevent unrestricted access. All campuses require extra security staffing at public or special events. Every campus also provides general safety and security education and violent crime awareness training to faculty, staff, and students.

In order to reduce the threat of workplace violence, most campuses have comprehensive workplace violence prevention and response programs that include multi-disciplinary behavioral risk assessment and response teams. Campuses have also established related programs for complaint resolution, employee and student assistance and counseling, and sexual harassment. Campuses provide workplace violence training and education for staff, supervisors, faculty, and students. These programs typically cover prevention, early detection and intervention, conflict resolution/mediation, supervisory response, policies, referral/response procedures, and anger/stress management, as well as general personal safety and security.

There are also a number of administrative, management, and supervisory controls and procedures in place to prevent, assess, mitigate, and respond to potential workplace violence. Some campuses have established "Zero Tolerance" policies in accordance with "Principles of Community." At least one campus has instituted "Quality Hiring Practices" that include screening, checking references, background checks, and avoiding the use of temporary or outsourced labor. Some campuses perform background criminal checks on all new employees. UC Police Departments have developed campus wide security plans and sponsor escort programs for nighttime safety.

Legal issues

Among the concerns that emerged in the wake of the Virginia Tech tragedy is whether public safety is endangered by constraints imposed on universities by the Federal Educational Rights and Privacy Act (FERPA) of 1974, which is intended to protect the confidentiality of student records and define under what circumstances parents can have access to student information and grades.

The University of California shares concerns that FERPA's definition is vague and open to interpretation. UC campuses' own practices, under certain circumstances, have broadly interpreted FERPA, with the result that information regarding a student's mental health has sometimes been released to parents or guardians in the hope of preventing suicides, assaults and other crimes.

Appendix A. President Dynes' Letter to The Regents and Charge Letter to Members of the Task Force

The University of California believes it is appropriate to explore legislative remedies that would clarify FERPA by more clearly defining circumstances universities can release information to parents; would "hold harmless" universities that, after consultations with qualified mental health professionals and acting in the best interest of the student, release information to parents or guardians; and would provide options for involuntarily withdrawing a student, without violating disability laws, then the institution reasonably determines, after making an individualized assessment, that the student poses a direct threat to himself.

Communications preparedness

Based on the campus responses to the University of California's annual emergency preparedness survey, nearly all of the UC campuses have some type of campus-wide emergency notification system. Keep in mind there is no single solution or universal technology – a multi-pronged approach is necessary to reach the entire campus community.

The most common notification systems at UC campuses include:

1) Broadcast email messages

2) Web page (Campus home page emergency messages)

3) 800# toll-free emergency hotline

4) Portable P.A. system (police car loudspeakers)

In addition, some campuses have other/additional systems including:

1) Reverse-911 phone notification (initiated by UCPD dispatch center)

2) Campus-wide siren/public address systems

3) Campus radio station and/or television station emergency broadcasts

Many campuses also have "Building Coordinator" programs where there is a single point of contact at every campus building whose responsibilities include emergency notification, response, and reporting back to the Campus PD or EOC (Emergency Ops Center) by either phone or handheld radio. Other communications approaches continue to be studied.

Appendix A. President Dynes' Letter to The Regents and Charge Letter to Members of the Task Force

UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO   SANTA BARBARA • SANTA CRUZ

OFFICE OF THE PRESIDENT

Robert C. Dynes
President

1111 Franklin Street
Oakland, California 94607-5200
Phone: (510) 987-9074
Fax: (510) 987-9086
http://www.ucop.edu

May 3, 2007

PROVOST HUME
EXECUTIVE VICE PRESIDENT LAPP

Dear Rory and Katie:

Thank you for agreeing to Co-Chair the new UC Campus Security Task Force that will study how our campuses can enhance their security, notification processes, mental health services, and general preparedness.

I ask that the Task Force devote substantial time over the next 60 days to address these critical issues facing the University and higher education and to then make recommendations to the Chancellors and me. I recognize that considerable work has already been done in a number of these areas, including student mental health and emergency preparedness, so I ask that your efforts be reviewed in light of what we have learned from the recent Virginia Tech tragedy. In addition, I am asking that the group explore additional legal or legislative remedies that could improve the balance between privacy and security protections, particularly with respect to the proper University notification of parents when mentally ill students threaten violence against themselves or others.

I deeply appreciate your willingness oversee this important effort. I enclose a copy of the letter I have sent inviting individuals to serve on the Task Force for your information.

Sincerely,

Robert C. Dynes

Enclosure

Appendix A. President Dynes' Letter to The Regents and Charge Letter to Members of the Task Force

UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO   SANTA BARBARA • SANTA CRUZ

OFFICE OF THE PRESIDENT

Robert C. Dynes
President

1111 Franklin Street
Oakland, California 94607-5200
Phone: (510) 987-9074
Fax: (510) 987-9086
http://www.ucop.edu

May 3, 2007

UNIVERSITY COUNSEL BIRNBAUM

Dear David:

Along with the national grief that has followed in the wake of the tragic shootings at Virginia Tech University have come questions about what can be done to prevent such a rampage from ever happening on a University of California campus.

To help answer those questions, I am asking you to serve on a new UC Campus Security Task Force to study how the University of California campuses can enhance their security, notification processes, mental health services, and general preparedness. The Task Force will be co-chaired by Provost Rory Hume and Executive Vice President Katherine Lapp, and will be composed of a broad-based group of other University security, student affairs, legal, and emergency preparedness experts. The enclosed overview shows that the University of California has many sound practices, policies and systems in place, however, it is clear there is room for improvement.

I ask that the Task Force devote substantial time over the next 60 days to address these critical issues and to then make recommendations to the Chancellors and me. I recognize that considerable work has already been done in a number of these areas, including student mental health and emergency preparedness, so I ask that these efforts be reviewed in light of what we have learned from the Virginia Tech experience. In addition, I am asking the group to explore additional legal or legislative remedies that could improve the balance between privacy and security protections, particularly with respect to the proper University notification of parents when mentally ill students threaten violence against themselves or others.

There can be no greater priority than the safety of the University of California's students, faculty and staff. While UC can take pride in the many positive and proactive steps we have taken over the last several years, the Virginia Tech tragedy underscores that more can always be done to make our campuses safer and more secure, as well as less vulnerable and more resilient in the aftermath of any extraordinary disruption.

SAME LETTER SENT TO THOSE ON ATTACHED LIST

Appendix A. President Dynes' Letter to The Regents and Charge Letter to Members of the Task Force

Please let Mrs. Maria Barros-Lee here in the Office of the President know of your availability and willingness to serve on the UC Campus Security Task Force by May 11. She can be reached by e-mail at maria.barros-lee@ucop.edu. Provost Hume and Executive Vice President Lapp will be in touch with the members soon to schedule the first meeting.

Sincerely,

/s/ Robert C. Dynes

Robert C. Dynes

Enclosure

cc: Provost Hume
        Executive Vice President Lapp
        Mrs. Barros-Lee

Appendix B. Selected Virginia Tech Reviews

The workgroup reviewed the work of other organizations in assessing their emergency response capabilities relative to the Virginia Tech event. Of particular interest were the:

- **Information and Communications Infrastructure Presidential Working Paper (Virginia Tech Telecommunications Working Group – August 2007):**
http://www.vtnews.vt.edu/documents/2007-08-22_communications_infrastructure.pdf

- **Security Infrastructure Presidential Working Paper (Virginia Tech Security Infrastructure Working Group – August 2007):**
http://www.vtnews.vt.edu/documents/2007-08-22_security_infrastructure.pdf

- **Interface Group Presidential Working Paper (Virginia Tech Interface Between Counseling Services, Academic Affairs, Judicial Affairs and Legal Systems Working Group – August 2007):**
http://www.vtnews.vt.edu/documents/2007-08-22_internal_communications.pdf

- **Mass Shootings at Virginia Tech – Report of the Review Panel to Governor Kaine, (Commonwealth of Virginia – August 2007):**
http://www.governor.virginia.gov/TempContent/techPanelReport.cfm

- **Florida Gubernatorial Task Force on University Campus Safety – May 2007:**
http://www.dcf.state.fl.us/campusSecurity/finalReport.shtml

- **Report to the President on Issues Raised by the Virginia Tech Tragedy (Federal Department of Health and Human Services, Department of Education, and Department of Justice – June 2007):**
http://www.hhs.gov/vtreport.html

- **Effective Disaster Warnings report (National Science and Technology Council – November 2000):**
http://www.sdr.gov/NDIS_rev_Oct27.pdf

Appendix C. Student Mental Health Committee Final Report

To be included without appendices in the hard-copy Campus Security Task Force Final Report; the full Student Mental Health Committee Final Report (including appendices) may be found on-line at:

http://www.ucop.edu/sas/student_affairs_and_services/SMHCommittee2006.pdf

Appendix D.   Systemwide Summary: Provisional Campus Blueprints for Implementation of the Student Mental Health Committee Report Recommendations

Blueprints for implementing the Student Mental Health Report recommendations were developed by campus Student Affairs divisions, in response to a request from Interim Vice Provost Joyce Justus in December 2006. The request was made on the assumption that additional resources could be made available (either over a single year or over a period of several years) up to the level of the full 25% net increase to the Registration Fee that was earlier recommended by the Vice Chancellors for Student Affairs, and endorsed by Provost Hume, for the initial cycle of funding of these needs. This level of increase would yield approximately $38,000,000 in additional programmatic revenue across the system (based on a systemwide enrollment figure of approximately 205,000 students). Therefore, the dollar amounts associated with some of the recommendations below (particularly in Tiers 2 and 3) are not necessarily reflective of the full magnitude of the campus need, but are projections rather of those portions of the campus need that might realistically be funded within the general level of resources ($38,000,000) potentially available to campuses for this purpose over the years immediately ahead. Please also note that the below estimates are provisional, and are subject to further adjustment both as campus needs assessments continue to be refined, and as ongoing consultation occurs with campus Student Fee Committees and others who play a key role in campus allocation processes.

Tier 1

T1-1	**Increase mental health staff (104.5+ FTE)**	**7,917,103**
T1-2	**Increase mental health staff salaries**	**1,489,912**
T1-3	**Increase disabilities services staff (16.5+FTE)**	**1,213,278**
T1-4	**Strengthen student judicial services (14+ FTE)**	**774,189**
T1-5	**Strengthen campus crisis response capacity (6.5+ FTE)**	**467,576**
T1-6	**Strengthen case-management capacities (7+ FTE)**	**542,238**
T1-7	**Strengthen ties with academic medical centers**	**60,000**
T1-8	**Re-evaluate counseling centers business models**	**92,400**
T1-9	**Best-practices development and implementation**	**130,000**
T1-10	**Develop systemwide reporting mechanisms (5.5+ FTE)**	**687,506**
	Tier 1 Sub-total (154+ FTE)	**13,374,202**

Tier 2

T2-1	**Integrated prevention programs (10.5+ FTE)**	**1,174,679**
T2-2	**Targeted intervention programs (18+ FTE)**	**1,677,881**
T2-3	**Restore staffing levels of impacted services (72+ FTE)**	**3,908,790**
T2-4	**FTE Parent outreach (2+ FTE)**	**174,700**
T2-5	**Strengthen Counseling/residential life partnerships (5+ FTE)**	**556,204**
T2-6	**Web-based services/hotlines (1+ FTE)**	**382,000**
T2-7	**Develop mental health student peer advisors (4+ FTE)**	**679,314**
T2-8	**Develop post-vention procedures**	**65,000**
	Tier 2 Sub-total (112.5+ FTE)	**8,618,568**

Tier 3

T3-1	Expand key academic support learning services (29.5+ FTE)	1,759,173
T3-2	Promote student well-being through enhanced activities (33.5+ FTE)	2,910,703
T3-3	Institute campuswide mental health awareness Programs (1+ FTE)	305,000
T3-4	Augment support for faculty involvement in student groups (2+ FTE)	190,600
T3-5	Student Affairs/Academic Senate partnering (1+ FTE)	63,100
T3-6	Mentoring training for graduate student advisors/faculty (1+ FTE)	127,500
T3-7	Review policies for negative impact on international students (0.5+ FTE)	90,000
T3-8	Establish periodic systemwide mental health conference	110,000
T3-9	Conduct annual campus review of student mental health issues	57,000
T3-10	Work with Academic Senate to advise and mentor students experiencing academic difficulty	<u>100,000</u>

Tier 3 Sub-total (68.5+ FTE) <u>5,713,076</u>

Tier 1 + Tier 2 + Tier 3 Subtotal (335+ FTE) <u>27,705,846</u>

(Please note that all new FTE salary costs above are exclusive of benefits, supplies and equipment, and space costs; see campus estimates of these aggregate additional costs immediately below)

Additional FTE costs (benefits, equipment and supplies, space) not included in above estimates:

Benefits:	6,276,709
Equipment/Supplies	1,854,975
Space	<u>5,702,548</u>

<u>13,834,232</u>

GRAND TOTAL <u>41,540,078</u>

Appendix E. Preliminary Guidelines for Campus Crisis Communication Plans

I. Introduction

A campus Crisis Communication Plan should include the purpose, intent, and scope of the plan, including information on when and how the plan will be activated. Typically, the plan would address most of the following considerations.

II. Anticipating a Crisis

Emphasize the importance of periodic assessments and exercises to identify and evaluate existing and potential campus risks/threats. Anticipate worst-case scenarios of all possible crises, and be prepared for how the media and the public will react to news of a crisis.

III. Preparing for a Crisis

1. Define and identify campus-wide mass notification systems and how to activate them.
2. Establish a Crisis Communication Team. The team should consist of pre-designated University officials with clearly defined roles in activation and execution of this plan.
3. Maintain current contact information for the Crisis Communication Team and key officials (including local/statewide public governmental institutions).
4. Identify the location of a command/media Department Operations Center (DOC) or Joint Information Center (JIC). This facility can be co-located with the Emergency Operations
5. Center (EOC) and might include a work space for reporters and a place to conduct press briefings.
6. Prepare a standby statement and pre-scripted messages**.** A general statement and messages for expected crises should be drawn up and approved in advance. Accurate details can be inserted at the time of the event.
7. Compile a media crisis kit. The crisis kit should contain all of the above items and lists along with directories, phone books, media lists and phone numbers, several legal pads, pens, maps, press badges, letterhead on electronic format for press releases, and possibly two-way radios and a laptop computer.
8. Communicate this plan in advance. This plan should be communicated to the media and to the University community before a crisis occurs.

IV. Identifying a Crisis

Different types of crises call for different responses. For example:

- An immediate unforeseen crisis with either many lives at risk/lost *(examples: earthquake, large fire, flood, terrorist attack, chemical spill)* or individual lives at risk/lost *(car accident, homicide/suicide, small fire, disease outbreak)*
- An ongoing crisis that increases in scope and impact as more information becomes known *(Examples: sexual harassment lawsuits, scandals)*

- An unusual, unexpected crisis or critical incident that does not fit into the above categories *(Example: Virginia Tech)*

V. Handling a Crisis

When crisis strikes, it is essential that the University take immediate action. The following steps should be taken as soon as the crisis is identified:

Action:
- o Activate the Emergency Operations Center (EOC) if necessary. Report to the EOC Director/Manager and coordinate all actions and messages through the incident management team.
- o Gather and assess the facts.
- o Convene the Crisis Communication Team.
- o Activate the Crisis Communication Plan.
- o Prepare a statement and background information. Tailor the pre-scripted messages to the events, and prepare background information for the media.

Communication:

- o Identify key audiences. Determine who needs to be informed of the situation, and in what order (both on and off campus).
- o Designate a university spokesperson(s).
- o Coordinate with the local Joint Information Center if the event is regional (not confined to the campus).
- o Provide guidance to the campus and community as developed by the EOC or Crisis Communication Team (if the EOC is not activated).
- o Activate all available and/or appropriate mass notification systems to communicate the message**.**
- o Develop additional messages to be delivered repeatedly and clearly and by one voice.
- o Control the message and the flow of information.
- o Keep track of all calls and requests with a contact log.
- o Respond to the media quickly and fairly.
- o Manage rumors and misinformation.

VI. Considerations

- o Set good policy.
- o Meet ethical responsibilities.
- o Choose words and phrases carefully.
- o Plan for FEMA reimbursement.

VII. Post-event Assessment

After the crisis is over, evaluate how the University handled it. Participate in the debriefings and EOC After-Action reports. Convene the Crisis Communication Team after the incident to evaluate actions taken and revise the plan as necessary.

Campus Crisis Communication Plan Appendices

A. Campus Alerting & Warning emergency notification procedures
   a. All systems available on campus
   b. How to access and activate systems

B. Key contact list

C. Campus Crisis Communication Team membership

D. Department Operations Center / Media Center locations

E. Pre-approved standby statement and pre-scripted messages

F. Media crisis kit

Appendix F. <u>University of California Campus Mass Notification Systems</u>

This information was gathered by querying emergency managers at each campus. It summarizes the types of emergency mass notification systems currently in place at all campus/medical centers as well as enhanced/advanced capabilities and systems mentioned by each campus.

Systems Common to all campuses	1. Mass e-mail to campus accounts 2. Broadcast voice-mail to campus phone (except UCLA & UCSD MC) 3. Emergency webpage(s) or home page banner (except Med Centers) or link on all campus pages 4. Emergency hotline/call-in number (toll-free or not) 5. Mobile PA system (generally in UCPD cars, sometimes hand carried)
Also common to Medical Centers	1. Overhead Public Address system 2. Text pagers

Enhanced/Advanced Capabilities/Systems:	
Berkeley	Outdoor alerting system (siren) with published procedures Campus FM radio station Campus hotline call center (10 phones) Opt-in desktop popup for campus computers
Davis	Student radio station Cable TV override Mobile traffic message signs
Irvine	Campus FM radio station E-messages to technology enabled (Smart) classrooms Automated SMS/text messaging system (ZotALERT)
Davis Med Ctr.	CAHAN (text system from State HHS, contacts 200 personnel) Vocera (wireless voice communications for 4000 staff)
Los Angeles	Cable TV override Campus AM radio station Panic alarm system in one administration building Outdoor emergency notification system
Merced	Message screens in library Limited inside PA through fire annunciator panels
Riverside	Student radio station
Santa Barbara	Student radio station AM radio station Mobile traffic message signs
Santa Cruz	Student radio station "Reverse 911" notification system – limited use
San Diego	CityWatch "Reverse 911" – limited use Connect-Ed (automated text/SMS system for text/voice)
San Diego Med Ctr.	Vocera (wireless - limited use) CityWatch "Reverse 911" (for about 20 administrative leaders)

Appendix G. Emergency Communications Gap Analysis - Campus Example

Following is an excerpt from a comprehensive campus gap analysis developed to document the campus' assessment of their emergency management and response program, including police, fire, emergency management, EH&S, IT services, and risk management. Campuses should conduct such gap analyses.

Category of Analysis	Current Service and Program	Best Practice Recommendation for Service and Program Preparedness	Gap Analysis and Key Considerations/ Challenges	Action Item	Due Date	Funding Required	Priori ty	Owner
Info Technology :								
VoiceMail Broadcast message	▪ Time to activate: 15 min ▪ 66 simultaneous calls into the system. ▪ Can be activated remotely	▪ Use only in an emergency situation and in conjunction with other notification processes. ▪ Keep message as brief as possible	▪ Low value - will not cause the phone to ring or message light to flash. ▪ Only works on land lines with activated voicemail boxes. ▪ Currently only used by Telecom. Current staffing is 8-5 M-F. ▪ Relies on communications building infrastructure being in place to operate	▪ None	▪ None	▪ None	▪ L	▪
Reverse 911	▪ Can initiate concurrently 400 calls per hour ▪ Can be activated remotely	▪ Create standard message text for optional use in emergency situation ▪ If funding allows, pursue options to reduce notification time. ▪ Keep message as brief as possible	▪ Majority of students use cell phones instead of land lines. ▪ Need to obtain phone #s for locations outside campus telephone system. ▪ Need to obtain and update a current record of student cell #'s. ▪ A message will be left	▪ Provide training for emergency personnel and PIO ▪ Perform test to 1,000 campus phone #s. ▪ Obtain external campus telephone #'s from ▪ Obtain cell phone #'s from Student Affairs	▪	▪ Optional subscription service could reduce message delivery time from 4 hours to 1.5 hours :$1,000/year plus long distance	▪ H	

Category of Analysis	Current Service and Program	Best Practice Recommendation for Service and Program Preparedness	Gap Analysis and Key Considerations/ Challenges	Action Item	Due Date	Funding Required	Priori ty	Owner
			but for analogue lines NO message light will be flashing. ▪ Current database information not accurate for specific locations. ▪ Training will be required for anyone responsible for activating system. ▪ Fire department and dispatch will provide active notification lists. ▪ Relies on communications building infrastructure being in place to operate			charges (@ 10 cents/ call) $4,500 one-time cost to share notification with other campuses		
Blue Light Emergency Phones	▪ 46 Blue Light phones ▪ Additional 7 to be installed	▪ Consistent signage at all locations ▪ Campus training/awareness of emergency phone locations and use. ▪ Quarterly testing to verify lines are in working order.	▪ Signage indicates "Telephone" which creates confusion as to whether is for regular or emergency use. ▪ Relies on communications building infrastructure being in place to operate	▪ IT to coordinate with vendor and sign shop to update signage ▪ Spring testing to be scheduled	▪ Fall Q ▪ Test: 6/1/07	▪ Waiting for quote ▪ $200 per quarter for testing	▪ H	▪
Email Broadcast Message	▪ Mail Broadcast Message	▪	▪ Takes 45mins to deliver all messages. ▪ Recipients need to have access to device to read mail. ▪ Not everyone is on	▪	▪	▪ No additional funding required	▪ H	▪

Category of Analysis	Current Service and Program	Best Practice Recommendation for Service and Program Preparedness	Gap Analysis and Key Considerations/ Challenges	Action Item	Due Date	Funding Required	Priori ty	Owner
			email system and they would need to have "Forward" implemented.					
Email Text Message	▪ Mail Text Message -most cell phone providers have email to TXT capability	▪	▪ Need to have current cell #'s/email addresses. ▪ Need to maintain current database of current contact data ▪ Could be slow and has not been tested for speed.	▪ No means to verify delivery of messages ▪ Dependent on external email delivery systems ▪ Subject to external site filtering, blocking and rate limits	▪	▪ No additional funding required	▪	▪
800 Megahertz Radio System	▪ Campus units rely on this as a redundancy system if voice communications fail. ▪ Can be administered from off-site	▪ Anyone using radios needs to go through training. This training should be refreshed every 3 years	▪ Valuable but vulnerable tool ▪ Campus terrain has dead spots in some areas. ▪ Trunking system allows for scalability required for several campus units to use system simultaneously. ▪ Current system not fully supported by vendor. ▪ No budget to replace this system. ▪ For internal use only ▪ Relies on infrastructure being in place to operate	▪	▪	▪	▪	▪

Appendix H. Overview of Mass Notification System (MNS) Technology Solutions

Audible systems

- **AM or FM Radio** (alert user of a crisis or warning)
    - o **Satellite-based Radio** (uses satellite technology to broadcast alerts or warnings to a subscription service area)
    - o **NOAA Weather Radio** (audible warning system uses tone alert decoded signal to alert user of crisis or warning)

- **Public Address Systems**
    - o **Audible Voice/Tone Platforms** (outdoor audible warning system using voice/sound)
    - o **Mobile** (vehicle-mounted speakers used by emergency vehicles to convey warnings)
    - o **Portable** (handheld bullhorns used to convey audible warnings)
    - o **Fixed** (indoor or outdoor, activated from central location)

Visual Systems

- **Changeable Message Signs (CMS)** on freeways and on some city/local arterial roads (subject to first priority of use for traffic incidents) – currently used for Amber Alerts and centrally controlled from a Transportation Management Center (TMC)
- **Electronic Message Board** (LCD or LED based scrolling visual warning message system)
- **Flashing beacons and strobe lights –** wireless, uses a radio transmission (encode/decode) to activate a visual warning system
- **Closed circuit television systems (CCTV) –** monitors installed in buildings

E-Technology Based Systems

- **Mass e-mail system** (network notification system)
    - **Subscription-based mass e-mail system** (system targeted to registered users/subscribers)
    - **Network Banner or "Pop Up"** (network message box sent to user computer screen)

- **Mass voice mail system** (delivery to voicemail boxes within system)
    - **Reverse 911 phone dialer** (automated calling message system - uses phone data from a Public safety answering point [PSAP] aka dispatch center)
    - **Enhanced 911** (campus cellular calls directed to UCPD vs. CHP)
    - **Telephone Emergency Notification System (TENS) Auto-Dialer** (phone-based mass callout system)

- **Text Message Relay System** (email, wireless pager, PDA, text messaging, landline, mobile phone, satellite phone, TDD/TTY, fax, and two-way SMS)
    - **Geographically Targeted Messaging (GTM)** (identify a geographic target boundary

and text messaging is sent to receivers (i.e.: cellular users) in the grid)
- **Pagers –** receivers carried on the person that emit sound/vibration, and text or audible messaging

- **Indoor wireless speaker and visual system** (visual/audible warning system)

- **Radio Data System (RDS)** – uses special receivers targeted for special populations: schools, government agencies, etc. usually used in conjunction with a local FM radio broadcaster.
- **Emergency Alert System (EAS)** - local/federal emergency warning system using CAP and SAME technologies to transmit warnings from the local, state, and federal government. (radio/television-based visual/audible)
- **Radio over Internet protocol (ROIP) -** operates using transport protocols designed for the Internet (TCP/IP, UDP, etc) on private, wide area or local area networks to transmit data communication between a land mobile radio and computer, telephone, handheld PDA, etc.   May use a push-to-talk feature (PTT).
- **Voice over Internet Protocol (VOIP)** - operates using transport protocols designed for the Internet (TCP/IP, UDP, etc) on private, wide area or local area networks to transmit voice and data to user.
- **Seismic Warning System** - (uses "p" wave technology to send an alert of impending earthquake, may activate other warning systems)

Appendix I. Pros and Cons of Selected Mass Notification Systems

RADIO			
campus station	local campus controlled stations, FCC license or student station	▪ alerts local area; ▪ local control ▪ message could repeat continuously	▪ limited to listeners
commercial station	local commercial AM or FM stations	▪ alerts regional area; requires coordination with provider	▪ limited to listeners
VOICE/TONE			
audible voice/tone platforms	fixed outdoor audible warning system using voice/sound	▪ alerts wide area, ▪ can awaken citizens ▪ warns people outside ▪ can be activated remotely	▪ could encourage going outside instead of sheltering inside ▪ voice could be difficult to hear ▪ noise control ordinances
mobile	vehicle mounted speakers used by emergency vehicles to convey warnings	▪ can warn specific areas	▪ takes time to warn larger area ▪ requires available personnel
portable	handheld bullhorns used to convey audible warnings	▪ can warn specific areas	▪ takes time to warn larger area ▪ requires available personnel
public address systems	voice messages delivered over speakers	▪ cost effective if already installed ▪ quickly activated ▪ can deliver instructions	▪ notifies area where installed ▪ retrofitting can be very expensive
VISUAL			
changeable message signs	LCD or LED-based scrolling visual warning system	▪ changeable message ▪ could be moved to multiple locations	▪ cost to purchase new ▪ time to move into place and initiate
ELECTRONIC			
automatic notification systems	designed to reach large numbers of subscribers across multiple delivery channels with targeted messages.	*can include systems indicated with * below*	▪ can be expensive to purchase and integrate ▪ cost usually based on number of contacts or uses

mass email messages	campus network notification system	▪ quickly activated ▪ already available on most campuses	▪ only notifies current users ▪ network delays in delivery
*subscription based mass email	system targeted to registered users/subscribers	▪ quickly activated	▪ requires subscription, costs based on number of uses ▪ only notifies current users ▪ network delays in delivery
*network banner or popup	network message box sent to user computer screen	▪ quickly activated	▪ only notifies current users ▪ pop-blockers on computers
mass voice mail	delivery to extensions and voice mail boxes within system	▪ quickly activated ▪ already available on most campuses	▪ only notifies if answered ▪ delivery to voice mail ▪ network delays in delivery or voice mail pickup
*reverse phone dialer	uses phone point data from telecom	▪ quickly activated	▪ requires subscription, costs based on number of uses ▪ only notifies if answered ▪ delivery to voice mail ▪ network delays in delivery or voice mail pickup
*text message relay system	email, wireless pager, PDA, text messaging, landline, mobile phone, satellite phone, TDD/TTY, fax, and two-way SMS	▪ quickly activated	▪ requires subscription, costs based on number of uses ▪ only notifies if read ▪ non-delivery based on coverage of carrier
pagers	receivers carried on the person that emit sound/vibration, and text or audible messaging	▪ quickly activated ▪ inexpensive cost and subscription	▪ only notifies carriers

radio data system (RDS)	uses special receivers in conjunction with a local FM radio broadcaster	- quickly activated - can deliver voice instructions - can deliver to targeted area	- notifies area where installed - retrofitting can be very expensive
voice over internet protocol (VOIP	operates using transport protocols designed for the Internet to transmit voice and data to user.	- quickly activated - can deliver voice instructions - can deliver to targeted area	- notifies area where installed - retrofitting can be expensive