RECORDS WORKING GROUP
TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The USA PATRIOT Act enhances the government's ability to obtain court orders and subpoenas for University records, as well as the scope and reach of these records requests. In most instances, the government must still present a lawfully issued court order or subpoena to gain access to University records. As such, the USA PATRIOT Act does not significantly change campus policies and protocols for responding to subpoenas, court orders and search warrants.

According to campus and University counsels, and to the Records Working Group's knowledge, the University has not received any subpoenas pursuant to the USA PATRIOT Act. The Berkeley campus nonetheless must be prepared to respond to these and other types of information requests in an appropriate and efficient manner. The challenge for the campus is to strike a balance between ensuring the privacy of students, staff, and faculty, while meeting its legal obligations.

The Berkeley campus is committed to protecting the privacy rights of all members of its community, while complying with federal and state laws that govern the appropriate disclosure of information from records. The USA PATRIOT Act, though imposing, does not alter that commitment.

The Records Working Group began its deliberations in February 2003 and met four times. The Group discussed and evaluated campus privacy and disclosure policies and protocols, records management issues, and effective methods of communicating to the campus community. In assessing the adequacy of current campus policies, procedures and protocols for the disclosure of records, the Records Working Group found that most current campus policies are adequate in responding appropriately to requests for information under the USA PATRIOT Act.

That said, the Records Working Group, in its deliberations, also found areas where campus-wide or systemwide policies and protocols are lacking or are in need of revision. The Group also raised issues that the campus should address in order to facilitate the campus's response to records requests. Accordingly, the Records Working Group offers the following eleven recommendations to the USA PATRIOT Act Steering Committee for consideration and action.

Recommendations

1. The campus should continue its current practice related to student records as reflected in Chancellor Berdahl's *Anti-Terrorism and Student Records* Deans and Directors memo, dated December 3, 2001 (see Appendix E).

2. Campus units and departments should contact the UCPD, who will work with the Office of the Registrar to assess emergency health and safety situations.

3. The campus should adopt a narrow definition of what constitutes a Health and Safety emergency. Departments should use it in making their assessments of potential emergency situations.

4. Though it remains appropriate to disclose confidential student information to law enforcement in connection with emergencies, the campus should be informed that the Health and Safety exception is significantly limited as defined below:

    - The exception applies to a specific situation that presents imminent danger to a student or others of the University community or to a situation that requires the immediate need for information from student records in order to avert or diffuse serious threats to the safety or health of a student or other individuals.

    - Disclosure must be narrowly tailored considering the immediacy, magnitude, and specificity of information concerning the emergency.

    - The Health and Safety exception is temporally limited to the period of the emergency.

5. The Steering Committee should approve as a campus-wide protocol the draft Health and Safety protocol found in Appendix J.

6. The Office of the President (OP) should collect, review, revise and present one specific site for "Guidelines for Access to Records" for access by all UC entities. This would include reviewing RMP-8, RMP-7 and RMP-10 (subpoenas) for any overlap and to ensure proper references to current systemwide policies. OP should also review RMP-9 - UC Guidelines for Access to University Personnel Records by Governmental Agencies Correspondence, in order to address any additional requirements due to the USA PATRIOT Act.

7. The campus should review its internal policies on background and security checks in light of the potential use of disclosed records under the Act.

8. Campus departments should adopt three best practices related to records management and retention exemplified by the campus libraries in light of the USA PATRIOT Act's records requirements:

    a. As is true with all records, it is good practice for any university enterprise to only collect the information that it requires to complete its job. With this in mind, records custodians should continually assess whether information that is being retained is necessary. If statistics are deemed necessary, where feasible they should be collected absent any personally identifiable information.

    b. A clear subpoena protocol should be established for campus departments to use in training staff on what to do when a subpoena of records is received. The campus should adopt as its standard, the protocol adopted by the libraries (see Appendix H).

    c. Other campus departments should adopt the same due diligence in ensuring that staff and patrons of their services are well informed as to the implication of the USA PATRIOT Act on records requests.

9. The campus should adopt the modifications to the Electronic Communications Policy to ensure compliance with the USA PATRIOT Act provisions (see Appendix I).

10. A campus administrative Records Management Department should be re-instituted. An excellent administrative candidate to take on this role would be the Chancellor's Communications and Resource Center (CCRC). Reporting to the Associate Chancellor/Chief of Staff John Cummins, the department's director would be charged with several duties.

11. The campus should develop a Records Management website.

II. INTRODUCTION

On October 26, 2001, President Bush signed into law the USA PATRIOT Act of 2001[1] in response to the September 11 terrorist attacks on the United States. The USA PATRIOT Act amends over 20 federal statutes, including laws governing criminal procedures, computer fraud and abuse, foreign intelligence, wiretapping, immigration, and student records. The amendments expand the authority of the government to gain access to business, medical, student, and library records, including stored electronic data and communications.

The signing of the USA PATRIOT Act raised immediate questions in the minds of many on the Berkeley campus concerning the extent of the new law's provisions, its effect on existing civil liberties, and how the Act might change existing policies and practices on the Berkeley campus. Specifically, attention was directed to policies affecting the privacy community members have all come to expect with respect to information the University maintains about them.

On January 24, 2003, Chancellor Berdahl appointed the Berkeley campus USA PATRIOT Act Steering Committee to oversee the campus's response to the Act. The Steering Committee, chaired by Executive Vice Chancellor and Provost Paul Gray and Academic Senate Chair Catherine Koshland, subsequently appointed two Working Groups, one of which was the Working Group on the Disclosure of Records. The Records Working Group membership and charge can be found in Appendices A and B.

The Records Working Group was asked to:

- Review existing campus policies, procedures, and standards governing the disclosure of records, and make recommendations for any necessary changes.
- Review campus protocols for responding to subpoenas and search warrants.
- Review campus protocols for disclosure of records under the "Health and Safety" statutory exemption.
- Recommend mechanisms for effectively informing the campus community of campus policies and procedures governing the disclosure of records.

The Constitution of the State of California guarantees an explicit and strong right to privacy. The federal government also requires that privacy be afforded to individuals in the way certain information is maintained about them by agencies such as universities. Thus, it should come as no surprise that the University of California's numerous policies and practices related to the records it maintains for members of its community reflect the nation's and the state's deep commitment to privacy.

Given the University's longstanding commitments to protect the right to privacy, it was with great interest that the Records Working Group undertook its study of the provisions of the new Act and its implications for access by the federal government to records maintained at Berkeley for all who study, live, and work here.

---

[1] The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" Act (P.L. 107-56).

This report constitutes the culmination of deliberations by the Records Working Group. The Records Working Group discussed existing campus disclosure policies and their adequacy in light of the USA PATRIOT Act provisions; identified outstanding issues that the campus needs to address; and formulated recommendations for consideration. In its deliberations, University Counsels Cynthia Vroom and Maria Shanle from the UC Office of the General Counsel provided valuable advice and counsel to the Records Working Group regarding pertinent provisions of the USA PATRIOT Act and how these provisions affect the University's records policies and procedures. The Group also received excellent advice and counsel from Assistant Chancellor-Legal Affairs Mike Smith. The Records Working Group extends its deep appreciation for their assistance in the preparation of this report.

The Records Working Group hopes that this report assists campus leaders in ensuring that the University meets its legal obligations as delineated in the USA PATRIOT Act, while at the same time ensuring that individual privacy rights are afforded to the extent allowed, and in the case of California required, by law.

III. ASSESSMENT OF CAMPUS RECORDS POLICIES, PROCEDURES AND PROTOCOLS

A. Disclosure of Records

Numerous federal and state statutes govern the disclosure of information from records that are maintained by the University. Chief among them are the federal Privacy Act, the federal Family Educational Rights and Privacy Act (FERPA), INS regulations, and, at the state level, the Public Records Act and the Information Practices Act. A related policy area is the use of electronic media to communicate, as reflected in the federal Electronic Communications Privacy Act. The University has implemented policies that reflect these statutory requirements and, in most instances, the University's best practices for implementing them.

Finding: In its evaluation of campus policies, procedures, and protocols, the Records Working Group found that, in general, the USA PATRIOT Act does not change the types of processes that law enforcement may use to obtain records maintained by the University. In general, it simply enhances their ability to obtain court orders or subpoenas for University records. Even with the enactment of the USA PATRIOT Act and its amendments, in most instances the government must still obtain a court order or subpoena in order to gain access to records.

Given the various types of records maintained by the University, this report will discuss the effect of the USA PATRIOT Act on each type of record briefly in turn.

1. Student Records

The Family Educational Rights and Privacy Act (FERPA) of 1974 is a federal statute that applies to educational institutions that receive federal funds under any program administered by the U.S. Secretary of Education. FERPA and University policy govern the disclosure of information from student records, and access to these records by the students to whom the records pertain. These policies define, among other things, what are and are not student records, what information can and cannot be disclosed, and to whom disclosures can be made. Student records are defined as all records, in any medium, that contain information directly related to a student and are maintained by the University or another group acting for it. In general, only "directory information" may be disclosed to third parties, absent a written authorization by the student, or another statutory exemption permitting disclosure.

University policies related to disclosure of information from student records, and implementing FERPA, can be found at: http://uga.berkeley.edu/uga/disclosure.stm and http://www.ucop.edu/ucophome/uwnews/aospol/toc130.html.

a. Student Records: Subpoenas and Court Orders

FERPA allows University officials to release student records absent a student's written authorization in specific circumstances noted in its implementing regulations. (34 CFR Part 99). One such circumstance is when a subpoena is issued.
The USA PATRIOT Act revised FERPA to allow a court, based on specific and articulable facts, to issue a court order requiring an educational institution to disclose to the United States

Attorney General, or his designee, student records relevant to a terrorism investigation. It also does not require the University to notify the student or keep a record of the disclosure, as otherwise required under FERPA. This protocol is the same as other *ex parte* subpoenas the University has received in other types of circumstances, normally criminal investigations.

The USA PATRIOT Act also permits the U.S. Attorney General, or his designee, to obtain a court order for the disclosure of "business records" (discussed below). Because the definition of "business records" is extremely broad, University student records could theoretically be requested pursuant to a business records court order, as well as a FERPA court order.

To the Records Working Group's knowledge, the Berkeley campus to date has not received any student record subpoenas pursuant to the USA PATRIOT Act's provisions (under either the FERPA or "business record" provisions).

As a legal matter, the campus Office of Legal Affairs and the University's Office of the General Counsel have advised that the University must comply with lawfully issued subpoenas, court orders, and search warrants. On November 21, 2001, Assistant Chancellor-Legal Affairs Smith informed the Chancellor's Cabinet that departments that receive a USA PATRIOT Act subpoena or court order follow an established protocol, and that the Assistant Chancellor-Legal Affairs review with and advise the Chancellor of all subpoenas and court orders issued under the USA PATRIOT Act before responding (see Appendix C).

Student Record Subpoena Procedure: Subpoenas and court orders should be served on the custodian of the requested record(s). Departments or units that receive a court order or subpoena for student records should refer the server of the court order or subpoena to the Office of the Registrar (OR). The Office of the Registrar, as the custodian of student records, processes the majority of subpoenas and court orders for student records. OR has established written procedures and protocols for responding to such court orders and subpoenas (see Appendix D). OR changed its protocol for responding to such requests, based on the December 2001 Chancellor's memo. OR, as well as other campus departments, should continue to follow established protocols for complying with the long-standing FERPA and University requirements that information from student records be provided when served with a lawfully issued court order or subpoena.

As noted in Chancellor Berdahl's *Anti-Terrorism and Student Records* Deans and Directors memo of December 3, 2001 (Appendix E), campus departments should notify the campus Office of Legal Affairs upon receipt of a USA PATRIOT Act court order. Campus staff should be guided by the advice of counsel, based on the December 3 directive that "while the USA PATRIOT Act does not require notification of students when their records are subpoenaed, the campus will notify students unless the subpoena or court order directs otherwise" (see Appendix E). Given that the University has not yet received any requests based on the USA PATRIOT Act and, therefore, it is uncertain what the exact language may be used on such subpoenas, it is vitally important that all campus departments seek advice from campus counsel before proceeding.

Note that a court order or subpoena may not necessarily contain the phrase "USA PATRIOT Act" – rather, it could simply list the statutory citation for the order. The specific statutory

citations for the FERPA and "business records" provisions, respectively, are: (1) Family Educational Rights & Privacy Act (20 U.S.C. 1232g(j)); and (2) Foreign Intelligence Surveillance Act of 1978, Sections 501-503 (50 U.S.C. 1861 et seq.).

Finding: Responses to subpoenas or court orders for student records pursuant to a USA PATRIOT Act should be coordinated with the Office of Legal Affairs and the Office of the General Counsel. As is true with other *ex parte* student record subpoenas, departments should not notify a student that a subpoena for the student's records has been issued, if explicitly noted in the subpoena.

b. Student Records: Health and Safety Disclosures

FERPA also permits the University to disclose confidential information from student records absent a student's written authorization "to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals." This exemption is known as the "Health and Safety" exception.

There is much room for judgment by a record custodian as to when exactly the Health and Safety exception applies. Immediately following the September 11 terrorist attack, over 200 colleges and universities used the Health and Safety exemption to disclose information from student records to federal officials. Subsequently, the Federal Family Compliance Office issued additional guidance for campuses on when the Health and Safety exemption should be used, dramatically limiting the scope of appropriate disclosures pursuant to this provision (see Appendix F).

Specifically, although it remains appropriate to disclose confidential student information to law enforcement in connection with emergencies, the campus should be informed that the Health and Safety exception is significantly limited as follows:

- The exception applies to a specific situation that presents imminent danger to a student or others of the University community or to a situation that requires the immediate need for information from student records in order to avert or diffuse serious threats to the safety or health of a student or other individuals.

- Disclosure must be narrowly tailored considering the immediacy, magnitude, and specificity of information concerning the emergency.

- The Health and Safety exception is temporally limited to the period of the emergency.

The Office of the Registrar and the UC Police Department (UCPD) have an established understanding as to how a health and safety emergency should be handled. The Records Working Group agreed on the importance of developing a written protocol for all campus departments to follow in the event that campus staff members are confronted with a health and safety situation.

Finding: To the Records Working Group's knowledge, no releases under the Health and Safety FERPA exemption related to terrorism investigations have occurred on the Berkeley campus.

The campus nonetheless should establish a written protocol for assessing a health and safety situation for student record disclosure purposes. A draft Health and Safety protocol has been provided for the Steering Committee's review, at Appendix J.

2. Business Records

The state Public Records Act (PRA) and Information Practices Act (IPA) generally govern access to and privacy of records that are maintained by the University. The PRA is a state statute that provides that every person has a right to inspect any public record, with specified exceptions. In general, any documents that the University possesses, whether hard copy or electronic, are public records subject to disclosure. Certain documents, such as confidential personnel records, medical records, and most police records are statutorily exempt from release under the PRA. The IPA governs the disclosure of information from business records maintained by state agencies, including the University, and generally prohibits the disclosure of personal information from those records without the individual's consent, unless another specific statutory exemption permits disclosure. University policy regarding the disclosure of and access to information from University records is contained in University Business and Finance Bulletin RPM-8 (http://www.ucop.edu/ucophome/policies/bfb/rmp8toc.html).

a. Business Records: Subpoenas

Like FERPA, the state Information Practices Act permits disclosure of personal information contained in University records in response to a lawfully issued court order or subpoena.

As is the case with student records, the USA PATRIOT Act allows the U.S. Attorney General, or his designee, to obtain a court order for the disclosure of any type of business record. The definition of "business records" subject to such a court order is extremely broad, and could include any record maintained by the University, including student records, police records, medical records, and library records. The definition even includes other "tangible things" in addition to records.

The USA PATRIOT Act authorizes a directive accompanying this special "business records" court order (unlike a subpoena or regular court order), stipulating that the record custodian not disclose the existence of the court order to anyone other than to those "necessary to produce the tangible things" requested in the court order. Therefore, pursuant to a court order under this provision (Foreign Intelligence Surveillance Act of 1978, Sections 501-503 (50 U.S.C. 1861 et seq.)), a records custodian should only disclose the existence of the court order to those necessary to carry out the records search that would be required by this type of information request. This permitted disclosure would include contacting campus counsel or the Office of General Counsel, in order to determine whether the court order is lawfully issued and what the lawful scope of the order is. This type of court order will state on its face that its existence must not be disclosed. It may not contain the phrase "USA PATRIOT Act," and therefore may need to be recognized by its statutory citation: (Foreign Intelligence Surveillance Act of 1978, Sections 501-503 (50 U.S.C. 1861 et seq.))

As with a subpoena or court order for student records, the University is legally obligated to comply with a lawfully issued subpoena or court order for business records.

i. Academic Personnel

Policies and protocols regarding the disclosure of information from academic personnel records are well documented and can be found in Appendix G. In its review, the Records Working Group noted that several systemwide policies are outdated in light of the USA PATRIOT Act and need to be revised.

Personnel Records Subpoena Process: Academic Personnel Office (APO) or the Office of Human Resources (OHR) handles access to personnel files and records. When the request involves non-confidential personnel information, the individual whose record is being accessed is notified of the request. As noted earlier, should academic personnel records be subpoenaed pursuant to the USA PATRIOT Act, the protocol established by the Assistant Chancellor-Legal Affairs in his November 21, 2001 memorandum to the Chancellor's Cabinet will be followed (see Appendix C).

Finding: In its review, the Records Working Group found that requests related to academic personnel files have adequate campus protocols in place in light of the USA PATRIOT Act requirements. This is not the case for systemwide Academic Personnel policies.

ii. Non-Academic Personnel

Policies on "access to personnel records" and the "release of information" are broadly treated in both *Personnel Policies for Staff Members (PPSM)* and Union contracts. The issue of access by public authorities to staff personnel files is specifically addressed in the *PPSM* and related University policies (RPM-8).

Union contracts, in contrast, generally focus on the employee's access to his or her own personnel file, rather than public access to those files. Most contracts, however, specify that only "authorized" personnel will have access to a personnel file. Such authorized personnel can include public agencies depending on the situation.

Under current procedure, "personnel, medical or similar files" requested pursuant to a subpoena or court order must be provided to the requestor. In addition, the individual to whom the records pertain must be notified unless law prohibits notification. This is not inconsistent with the general requirements of the USA PATRIOT Act.

Finding: Campus access and disclosure policies and procedures pursuant to non-academic staff personnel record conform to the requirements of the USA PATRIOT Act.

iii. Background Checks

Under the USA PATRIOT Act, employees who are already working in a particular position may be required to pass a newly initiated security check in order to continue working. Though only tangentially related to the Records Working Group's charge, members noted that the requirements under the USA PATRIOT Act appear to be in conflict with existing campus policy regarding background checks. It is the Working Group's assumption,

however, that this issue will be fully investigated by the Working Group on Research, in particular the need to review internal policies on background and security checks in light of the potential use of disclosed records under the Act for this purpose.

iv. Police Records

UC Police records are kept in accordance with applicable federal and state laws. California Government Code section 6254(f) governs access by the general public to information contained in law enforcement records. The California Information Practices Act governs the privacy of personal information contained in such records, while other statutes also specifically address the maintenance and release of police records. The UCPD will continue to be guided by these established laws and regulations and, thus, UCPD procedures will not change under the USA PATRIOT Act. However, note that UCPD records may be the subject of a "business records" court order as described above.

b. Library Records

Policies regarding the disclosure of and access to information from library records are addressed in University Policies (RPM-8), which reflects the University's obligations pursuant to the Public Records Act and the Information Practices Act. As the libraries have consistently been on the forefront of privacy, the *Library Bill of Rights* (http://www.ala.org/alaorg/oif/privacyinterpretation.html) also guides the libraries in the provision of services, materials, and programs.

i. Review of Practices

The Library collects and maintains private patron information, including circulation and borrower records and library server logs. The library protects the privacy of its patrons whenever possible and as required by law and policy. Though the Library is secure in its current practices, it is revisiting its policies in light of the USA PATRIOT Act.

One area that the Library will review is the issue of circulation records. To the Records Working Group's knowledge, the Berkeley Library has not received any USA PATRIOT Act requests for circulation records; other libraries, however, have received requests for these records. The potential availability of library circulation records pursuant to a USA PATRIOT Act "business records" court order (Foreign Intelligence Surveillance Act of 1978, Sections 501-503 (50 U.S.C. 1861 et seq.)) is of significant concern to librarians across the country. Library circulation records kept for the purpose of identifying the borrower of items available in libraries are exempt from PRA disclosure requirements. However, if these records are the subject of a lawfully issued court order or subpoena, the Library is legally obligated to disclose the requested information. And if the court order is a special "business records" order under the Foreign Intelligence Surveillance Act, the Library is not only legally obligated to disclose the information, but also may not disclose the existence of the order (as described above).

The Berkeley Library is working in concert with University-wide librarians to review library practices and policies to ensure compliance with USA PATRIOT Act provisions, while

maintaining privacy and sensitivity issues. Part of the Library's responsibility in managing collected information is in letting users know what the Library gathers and why. An informed public is better able to ascertain just how much they care to participate in practices in which records may be linked back to them. The Library is actively reviewing its procedures on how best to inform users on the Library's practices in this arena.

In light of the Act and the pervasiveness of technology in the Library's day-to-day work, the Library is in the process of examining the type and format of information collected; developing protocols to respond to law enforcement requests; training Library staff on the implications of the USA PATRIOT Act; and making available information to its users concerning their rights and how information is being used. The Library Technology Advisory Group has recommended a number of practices be implemented concerning how the Berkeley Library should keep records. Some of these practices are requirements of federal or state law, while others represent policies or policy recommendations of the University or the American Library Association. The Privacy Audit can be found at http://www.cdlib.org/libstaff/privacytf/privacy_audit.html.

Though much has been accomplished, the Library's current goals are to review and address its policies on retention of and access to all types of information. Decisions remain to be made regarding data, logs and records of all types (digital and paper) to be discarded or saved.

ii. Libraries: Subpoenas

Library Records Subpoena Procedure: Subpoenas and court orders for library records should be referred to the Library. All Library employees, including the Director and student and part-time staff, have received consistent guidelines on how to respond to a request from law enforcement (see Appendix H). The memo also included contact information should a staff member receive a subpoena or warrant.

The Library is developing training programs for all Library staff to learn about their rights and responsibilities concerning the USA PATRIOT Act. A campus representative has been working with a number of libraries on campus and will soon meet with the Heads of Circulation within the UC Library system to discuss how their work may be affected by the Act. In a few months, there will be a northern California session made up of lawyers from the Office of the President General Counsel's Office and a knowledgeable library expert. In the meantime, the Library is holding training sessions as needed.

Finding: The goal of the Library is straightforward: protect the privacy of its patrons whenever possible. The Records Working Group found that Berkeley's libraries, in concert with other UC Libraries, has made headway towards this goal. The Records Working Group commends the Library for taking a leadership role in educating its staff and patrons on their privacy rights, and in addressing issues such as circulation records. The Records Working Group is confident that the campus libraries will continue to improve and examine their procedures.

B. Electronic Communications Policy Protocols

The University's Electronic Communications Policy (ECP) establishes specific procedures for non-consensual access to electronic communications records of campus faculty, staff, students, or affiliates who have been granted use of the University electronic communications resources. The ECP applies whether the electronic communications record is stored on a server or on an individual desktop workstation.

Search Warrants, Electronic Surveillance, Wiretapping, and Related Provisions

When the USA PATRIOT Act was signed, numerous concerns were raised about the possible infringement the new law might have with respect to enhanced electronic surveillance the government could now undertake. The same concerns were raised on the Berkeley campus. In its review, University Counsel informed the Records Working Group that the new Act's provisions should generally be treated in the same manner as past requests by law enforcement for search warrant or subpoena purposes. Should a department or unit receive a search warrant or subpoena pursuant to the USA PATRIOT Act for electronic communications, it will follow the established protocol outlined in Assistant Chancellor-Legal Affairs in his November 12, 2001 memorandum (see Appendix C). Note, however, that these new provisions may not permit the University to guarantee the same level of privacy of electronic records as it has in the past, even where this established protocol is followed.

Authorization for Access to Electronic Records

The campus has well-established protocols for access to electronic data. Given the sensitivity of much of the data and the expense associated with retrieving it, the campus needs to revise its practices and inform the campus community on what to do in the event that the government seeks electronic data from a campus department. The Records Working Group felt, however, that the campus needs to adopt certain changes to existing protocol related to notification requirements, reporting requirements, and informing the campus community on the cost of retrieving data should a USA PATRIOT Act subpoena be issued for electronic records to ensure that the ECP is congruent with the provisions of the USA PATRIOT Act.

Finding: Procedures established under the ECP are explicit as to what should be done whenever a non-consensual request for electronic data is made. These procedures need to be modified to conform to the requirements of the USA PATRIOT Act as found in Appendix I.

IV. DISCLOSURES TO THE DEPARTMENT OF HOMELAND SECURITY (SEVIS)

The Student and Exchange Visitor Information System (SEVIS), which was established after the September 11, 2001 terrorist activities, is a Department of Homeland Security automated student tracking system from which all F and J visa documents will be produced. SEVIS implements the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) passed in 1996. This law requires the Immigration Service (since March 1, 2003 a part of the Bureau of Homeland Security) to collect current information, on an ongoing basis, from schools and exchange programs relating to nonimmigrant F and J students and J visiting scholars during their stay in the United States.

The 1996 legislation (IIRIRA), which mandated that every person issued an INS document be tracked, waives the privacy provisions of the Family Educational Rights and Privacy Act (FERPA) for F and J visitors. Schools and program sponsors are authorized and required to report information on F and J visitors that would ordinarily be protected under FERPA. However, the FERPA waiver is limited to that information required by the government to determine that the F or J visitor is maintaining status or otherwise required by regulation. Data required by regulation include: name, date and place of birth, country of citizenship, local residential address, current academic and program status, begin date of study or program activity, degree program, field of study, and date of completion of degree or program activity. Much of this information is public information under FERPA, while some is not. SEVIS does not affect the ability of the general public to access such information. SEVIS does, however, create a new method of creating travel documents for and monitoring of F and J students and visiting scholars.

Under SEVIS, the University will be required to: regularly report to INS the student arrival and enrollment dates; provide updated student contact information; and provide other student data, most of which are public information. This mandated data/tracking system provides the government a tool to monitor F and J visitors to ensure they are where they are supposed to be and doing what it is they were admitted to the U.S. to do.

The data elements required for document production, with the exception of address information, are generally the same elements schools and program sponsors have collected and provided on the forms issued to F and J visitors before SEVIS. The SEVIS system allows the government to have this information before the visit starts rather than after arrival. Until SEVIS, the government had no "real-time" information to verify that visitors, once admitted to the U.S., actually report to their schools/programs. Reporting the arrival of F and J visitors is now required of schools and program sponsors. Likewise, the government has not had a method of being informed that visitors are maintaining status or have ended their program/degree programs. The SEVIS system will now receive this information from schools and program sponsors.

Finding: The USA PATRIOT Act provisions are no different for F and J visitors than for any other person in the U.S. Access to information on F and J visitors, other than that which is permitted under SEVIS and consent given by students via the issuance of visa documents, requires the government to obtain a court order or subpoena. This is consistent with procedures that law enforcement must follow for information requests regarding U.S. citizens and permanent residents. This Act did mandate that the SEVIS system be "fully implemented and expanded

prior to January 1, 2003." The Records Working Group commends the SISS for taking a leadership role in the SEVIS process.

V. RECORDS MANAGEMENT ISSUES

Though the main focus of the Records Working Group was to ensure that current campus policies and protocols for responding to information requests are adequate and appropriate, the Working Group realized early on that navigating through the vast amount of information to locate policies was a difficult task even for well-seasoned managers who are quite knowledgeable about University policies and procedures.

Unlike other UC campuses, the Berkeley campus currently does not have a stand-alone department with campus-wide responsibility to deal directly with campus-wide records management matters. While a position existed in the 1980s that served in this capacity, its responsibilities have been delegated through ad hoc arrangements with various offices. It is the opinion of the Records Working Group that, though well intentioned, this has had a diluting effect on the authority for issuing campus-wide policy statements, best practices and protocols for responding to federal, state, and University records requirements. The absence of such an administrative unit at a high level creates a number of challenges for campus administration:

> First, no uniform records philosophy exists on campus. In the absence of such a philosophy, departments have developed their own idiosyncratic procedures whenever records issues arise. Those departments knowledgeable about University policies and procedures tend to do well; those who are not tend to make ad hoc decisions. The campus may be placed in a compromised position from a risk management perspective because of this.
>
> Second, no infrastructure exists to communicate records matters succinctly and accurately to staff. While the campus has great resources to call upon when decisions must be made with respect to the disclosure of information maintained in the myriad types of records maintained on campus, the Records Working Group feels it is safe to say that many able administrators do not know how or where to find the needed policy direction. The unfortunate result is that administrative units are now called upon to "reinvent the wheel" every time a records issue arises. There is no place to serve as a clearinghouse or resource to prevent this unfortunate waste of staff time and talent.

It is clear to the Records Working Group that the campus must better communicate to staff what to do upon receipt of a records request, and how to do it in light of the USA PATRIOT Act. The Working Group discussed mechanisms to improve the dissemination of policies and procedures so that the campus community can readily access campus polices. Deans and Directors memos are not sufficient in communicating policies to the entire campus community.

One example of this lack of campus-wide responsibility lies in the area of subpoenas. Though the Working Group found that existing policies were adequate in light of the new law, the Working Group was very troubled by the lack of campus-wide policies and protocols for complying with subpoenas, court orders, and search warrants. Solid and well-established campus-wide policies would help ensure the University responds to law enforcement requests consistent with all applicable legal requirements while protecting all privacy rights afforded under state and federal privacy acts.

A second example is the lack of a campus-wide understanding of the obligations for records retention and adequate stewardship of records. The Records Management Program (RMP) was established by UCOP in part to promote sound records management practices; to assure the protection of records vital to the University; and to establish and monitor a program of records disposition to assure that University records are not maintained longer than necessary, but are maintained as long as needed to meet administrative and legal requirements. The RMP series also includes disposition schedules for records classified by functions, including administrative, fiscal, medical, payroll/personnel/benefits, physical plant, student and applicant records, library, and administrative electronic data.

The current retention schedules are over ten years old. The Office of the President is in the process of revising the RMP and retention schedules. Until the revision is complete, the old schedules apply. Since the current RMP contains documents that no longer exist and does not include documents that were created after the last revision of the RMP, the Working Group believes that it is in the University's best interest to complete the revision of the RMP quickly. The campus should adopt interim schedules to ensure that record custodians maintain records appropriately.

A third example of this lack of campus-wide responsibility is the role of the IPA Coordinator, which has been housed in different divisions over the last decade. The RMP-7 requires a "Coordinator of Information Practices" on each campus. Currently, many campus units notify University Counsel upon receipt of a PRA or IPA request because who the Coordinator actually is at times is not fully understood by campus personnel. University Counsel (and other offices) must then step in and determine which office should respond to PRA or IPA requests.

Finding: The Records Working Group discovered that, with respect to non-personnel requests, there is currently no written procedure on how to respond to business record requests. The lack of a clear protocol distributed to campus units could result in untimely responses, increases the risk of inappropriate disclosure, and increases vulnerability to legal action. This has been highlighted with the introduction of USA PATRIOT Act and the University's obligations that flow from it.

Finding: The Records Working Group is concerned that, while some departments and units have individual policies and protocols, the campus does not have campus-wide protocols for handling subpoenas, search warrants, and health and safety emergency situations.

VI. CONCLUSION AND RECOMMENDATION

In light of its findings, the Records Working Group offers the following recommendations to the USA PATRIOT Act Steering Committee for its consideration and action:

Recommendation 1: The campus should continue its current practice related to student records as reflected in Chancellor Berdahl's *Anti-Terrorism and Student Records* Deans and Directors memo, dated December 3, 2001 (see Appendix E).

Responsible Entity: All Departments

Recommendation 2: Campus units and departments should contact the UCPD, who will work with the Office of the Registrar to assess emergency health and safety situations.

Responsible Entity: All Departments

Recommendation 3: The campus should adopt a narrow definition of what constitutes a Health and Safety emergency. Departments should use it in making their assessments of potential emergency situations.

Responsible Entity: The USA PATRIOT Act Steering Committee

Recommendation 4: Though it remains appropriate to disclose confidential student information to law enforcement in connection with emergencies, the campus should be informed that the Health and Safety exception is significantly limited as defined below:

- The exception applies to a specific situation that presents imminent danger to a student or others of the University community or to a situation that requires the immediate need for information from student records in order to avert or diffuse serious threats to the safety or health of a student or other individuals.

- Disclosure must be narrowly tailored considering the immediacy, magnitude, and specificity of information concerning the emergency.

- The Health and Safety exception is temporally limited to the period of the emergency.

Responsible Entity: The campus FERPA Compliance Officer (the Registrar)

Recommendation 5: The Steering Committee should approve as a campus-wide protocol the draft Health and Safety protocol found in Appendix J.

Responsible Entity: The USA PATRIOT Act Steering Committee

Recommendation 6: The Office of the President (OP) should collect, review, revise and present one specific site for "Guidelines for Access to Records" for access by all UC entities. This would include reviewing RMP-8, RMP-7 and RMP-10 (subpoenas) for any overlap and to ensure proper references to current system wide policies. OP should also review RMP-9 - UC

Guidelines for Access to University Personnel Records by Governmental Agencies Correspondence, in order to address any additional requirements due to the USA Patriot Act.

Responsible Entity: The UC Office of the President, following transmittal of Request by the USA PATRIOT Act Steering Committee

Recommendation 7: The campus should review its internal policies on background and security checks in light of the potential use of disclosed records under the Act.

Responsible Entity: The Office of Human Resources

Recommendation 8: Campus departments should adopt three best practices related to records management and retention exemplified by the campus libraries in light of the USA PATRIOT Act's records requirements:

a. As is true with all records, it is good practice for any university enterprise to only collect the information that it requires to complete its job. With this in mind, record custodians should continually assess whether information that is being retained is necessary. If statistics are deemed necessary, where feasible they should be collected absent any personally identifiable information.

b. A clear subpoena protocol should be established for campus departments to use in training staff on what to do when a subpoena of records is received. The campus should adopt as its standard, the protocol adopted by the libraries (see Appendix H).

c. Other campus departments should adopt the same due diligence in ensuring that staff and patrons of their services are well informed as to the implication of the USA PATRIOT Act on records requests.

Responsible Entity: All Departments

Recommendation 9: The campus should adopt the modifications to the Electronic Communications Policy to ensure compliance with the USA PATRIOT Act provisions (see Appendix I).

Responsible Entity: USA PATRIOT Act Steering Committee and IS&T

Recommendation 10: A campus administrative Records Management Department should be re-instituted. An excellent administrative candidate to take on this role would be the Chancellor's Communications and Resource Center (CCRC). Reporting to the Associate Chancellor/Chief of Staff John Cummins, the department's director would be charged to:

1) Develop protocols clearly outlining what a staff member needs to do whenever records requests are made on campus requests (be they FERPA, PRA, IPA, USA PATRIOT Act, or other) to ensure that the campus's best interests are served with respect to a clear understanding of the different protocols required for handling records requests.

2) Serve as a clearinghouse for records management information on campus.
3) Establish a website that provides clear directions/guidelines to campus units on responding to records requests. The website should include a list of offices/units and the records for which they are custodians.
4) Develop and approve campus protocols and procedures for complying with subpoenas, court orders, and search warrants. The Working Group suggests a single set of protocols which point to one process to determine "how to handle" records requests, similar to what the campus Library has established.
5) Coordinate all law enforcement information requests, including a campus-wide protocol for subpoenas and search warrants.
6) Establish campus fee structure(s) for photocopying documents when complying with records requests.
7) Serve as the Berkeley campus's "Coordinator of Information Practices."

Given the heavy workload inherent in these efforts, the new unit should be staffed adequately to serve as a campus-wide clearinghouse for information dissemination and as the office with primary responsibility for responding to records requests. Models that would be good to adopt are those established on the UCSF and UCLA campuses (see Appendix K).

Responsible Entity: Chancellor's Cabinet

Recommendation 11: The campus should develop a Records Management website**.** There are many policies and procedures on campus; however, disseminating that information or trying to locate specific policies may prove challenging. The campus must develop mechanisms for better communicating to staff policies, procedures, and protocols for the disclosure of information and the ability to link the different policies together. The Working Group envisions a well-advertised website that would:

- Educate all campus staff and faculty about privacy acts and other relevant laws, compliance requirements, and University and campus policies.
- Post all privacy and disclosure policies, procedures, and protocols.
- Create a campus-wide listserve.
- Provide the campus community with periodic updates.

Responsible Entity: The New Records Management Department and COIS

Appendix A

USA PATRIOT Act
Steering Committee's Working Group
On the Disclosure of Records
Membership

Members

Susanna A. Castillo-Robson, Registrar, *Chair*
Carolyn Capps, Principal Analyst, Office of Vice Provost – Academic Affairs and Faculty Welfare
Jacqueline A. Craig, Manager, IS&T
Ted Goode, Director, Services for International Students and Scholars
Pat Carroll, Captain, UCPD
Amy Kautzman, Head, Research, Reference, and Collections Doe/Moffitt Libraries
Patti Owen, Director, Academic Personnel Office
Valerie Ventre-Hutton, Employee Relations Manager, Human Resources
Suzie Park, At-large Graduate Student Representative

Also Attending

Rose Chan-Gee, Analyst, Office of the Registrar
Maureen Hogan, Administrative Specialist, Office of the Registrar
Rozanne Largent, Associate Registrar, Office of the Registrar

Appendix B

Revised March 20, 2003

January 16, 2003

Registrar Susanna A. Castillo-Robson, Chair
Manager Jacquelynne A. Craig, IS&T
Director Ted Goode, Services for International Students and Scholars
Director Patti Owen, Academic Personnel Office
Valerie Ventre-Hutton, Human Resources Representative
Head Librarian Amy Kautzman, Research, Reference, and Collections Doe/Moffitt Libraries
Suzie Park, Graduate Student-at-Large

With the passage of the USA PATRIOT Act ("Uniting and Strengthening America by Providing Appropriate Tools required to Intercept and Obstruct Terrorism") in October 2001 and additional steps being taken with the goal of enhancing the security of the United States, the Chancellor has appointed a Steering Committee to oversee the campus response to the Patriot Act and related legislation. As noted in the Statement in Support of Civil Liberties and Academic Freedom issued by the Divisional Council in December, 2001, "Striking the perfect balance between civil liberties and academic freedom and the desire to improve internal security is an enduring, complex and difficult challenge."

As co-chairs of the Steering Committee, we are appointing a Working Group on the Disclosure of Records in order to ensure that campus policies and procedures for responding to requests for disclosure of records are adequate and appropriate, and that the campus community is informed about our policies. The charge to the Working Group is to:

> Review existing campus policies, procedures, and standards governing the disclosure of records, and send us recommendations for any needed changes, including how the policies are administered. The Working Group should review campus protocols for responding to subpoenas and search warrants, and protocols for disclosure of records under the "health and safety" statutory exemption categories.
>
> Recommend mechanisms for effectively informing the campus about our policies and procedures governing the disclosure of records, with the goal of ensuring that policies are clear and accessible, and that members of the campus community can readily determine how to respond to requests for disclosure of records.

We would like the Working Group to complete its review and send us its recommendations no later than April 30, 2003. Assistant Chancellor—Legal Affairs Michael R. Smith and Chief of Police Victoria Harrison are available to consult with the Steering Committee. The Registrar's Office will provide staffing.

Paul R. Gray Catherine P. Koshland

Executive Vice Chancellor & Provost Chair, Academic Senate

cc: Assistant Chancellor Michael R. Smith
Chief of Police Victoria Harrison

Appendix C

November 21, 2001

To: Chancellor's Cabinet
From: MRS

Re: **Subpoenas and PRA Requests for Campus Records; Anti-terrorism Legislation; Release of Chancellor's Office Records; Office of Legal Affairs Assistance**

This memo regards recent legal developments governing release of records to federal law enforcement officers investigating suspected terrorism following the September 11th events (particularly the USA PATRIOT Act), the role of the Office of Legal Affairs (OLA) in handling such requests, the general campus and OLA procedures for responding to records subpoenas and California Public Records Act (PRA) requests, and the specific protocol for processing requests for Chancellor's Office records.

Although the press has reported nationwide increased law enforcement requests for university records following September 11th, this has not yet occurred here. Since any such request would raise new questions of legal interpretation, I have agreed to consult with OGC and other campus counsel before responding, in order to assure a Systemwide uniformity of approach. I've asked Registrar Susie Castillo-Robson and International Students and Scholars Services Director Ted Goode to let me know if they receive any demands for student or foreign student records related to anti-terrorism investigations. Would you please advise the records custodians and coordinators in your units to bring to my attention, for the near future, any federal law enforcement subpoenas or search warrants for records under their control (these may not be limited to student records but might also pertain to security, personnel, research, computer, or academic records).

Recent Federal Legislation

The Department of Education recently ruled that it would be permissible under the Family Educational Rights and Privacy Act ("FERPA") for institutions, in the absence of a subpoena, to provide student educational records to federal law enforcement agents investigating terrorism (pursuant to FERPA's "health and safety" exemption). Subsequently, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT") Act of 2001. On October 26th I distributed a memorandum summarizing its provisions that are likely to have a significant impact on colleges and universities. Basically, it amends a wide variety of laws, including FERPA. It enables the Attorney General to obtain a court order for the unconsented release of student records relevant to a terrorism investigation. The University need not make a record of such disclosures, as otherwise required under FERPA. It also expands existing law permitting federal agencies to collect information about foreign students. As a general matter, requests for student records

related to anti-terrorism investigations should now be accompanied either by a court order pursuant to the USA PATRIOT Act (which does not require notifying the student), or a regular subpoena (which does require that the institution attempt to notify the student, unless expressly prohibited on the face of the subpoena). The FERPA "health and safety" exception may still be used to release information in appropriate circumstances (investigations involving an imminent threat or similar urgency), but should not be relied upon in cases of routine anti-terrorism investigations.

The new legislation enhances the federal government's authority to intercept wire, oral, and electronic communications relating to terrorism, computer fraud and abuse. It authorizes the voluntary disclosure to law enforcement agents of the contents of electronic communications if the provider reasonably believes there is a health and safety emergency. It expands the scope of technology related information (including stored voice mail and Internet usage) obtainable through warrants, subpoenas, and court orders. It increases law enforcement Internet surveillance authority, and authorizes providers to permit law enforcement officials access to communications of computer trespassers without a warrant. It permits the FBI to seize certain records subject to a subpoena that expressly prohibits disclosure of the fact that the records were released (other than to persons necessary to produce the records). This last provision is particularly significant given our established practice of notifying students and employees when their records have been subpoenaed.

Again, given the significance of this new legislation, please bring to my attention, at least for the near future, any federal court orders, subpoenas or search warrants your units may receive in the context of an anti-terrorism investigation.

General Campus Procedures for Handling PRA Requests and Subpoenas for Records

Of course, most subpoenas and PRA requests the Campus will receive will be unrelated to the new legislation. The basic principles and standards under University policy for disclosing University records remain largely unchanged.

PRA Requests

Most of our records managers are familiar with the basic provisions of the PRA. They are contained in University's Business and Finance Bulletin RMP-8, which is accessible at: http://www.ucop.edu/ucophome/policies/bfb/rmp8.html

The general rule is that documents in the possession of the University (whether hard copy or electronic) are public records subject to disclosure. Certain documents, however, are statutorily exempt from release (i.e., confidential personnel records, medical records, trade secrets, attorney-client privileged communications, federally protected student records, etc.). The PRA requires a response to all written requests within ten (calendar) days of receipt. Where there are no potential confidentiality concerns the records unit should normally be able to copy and forward the documents within that time period. If the records are not easily retrievable, and it will take additional time to search for them (or to consult with counsel as to whether particular documents are exempt from disclosure), the response must indicate "the estimated date and time when the records will be made available."

A new statutory requirement relates to those cases where the Campus cannot comply with the request due to ambiguity. In the past, where the request was vague or unintelligible, it was permissible to either seek clarification or simply deny the request on the grounds that it failed to ask for an "identifiable record." Now, unless the refusal to comply is also based on a specific statutory exemption, the Campus must affirmatively "assist the member of the public [to] make a focused and effective request" by doing three things: "(1) Assist the member of the public to identify records and information that are responsive to the request or to the purpose of the request, if stated. (2) Describe the information technology and physical location in which the records exist. (3) Provide suggestions for overcoming any practical basis for denying access to the records or information sought."

If the determination is not to comply with the request, the response must state the reason why. That is, it must either indicate that the record does not exist, or state that it does exist and cite the applicable statutory exemption(s) justifying nondisclosure. Any questions about the application of a particular exemption should be discussed with Assistant Campus Counsel Monique Shay (642-1991). Specifically, all PRA requests that (a) are related to university litigation, (b) involve particularly sensitive classes of records (i.e., academic peer review records), or (c) raise significant new policy or legal questions, should be brought to Monique's attention. Where records are exempt, she can assist the department in preparing the written denial. To facilitate a prompt analysis of the records and timely response, pertinent documents should normally be collected before contacting OLA.

*** PRA Requests received by the Chancellor's Office**

Normally, PRA requests are sent directly to the relevant unit or custodian of records. At times, however, requests for records located elsewhere will be addressed to the Chancellor's Office. In this case, where the appropriate office of record is evident, the request will be forwarded by CCRC to that unit or department. Otherwise, the request will be forwarded to the Vice Chancellor in whose area the documents would most likely exist, who should direct the request to the appropriate records manager with a reminder of the time constraints. PRA requests for Chancellor's office records will be forwarded to John Cummins, who is the designated Records Coordinator for this office. John will consult with me or Monique about the legal status of particular documents.

*** Records Subpoenas**

There are two types of subpoenas for records. A subpoena *duces tecum* is an order to produce particularly described records; it may also require the custodian of records to testify as a witness. A deposition subpoena relates to the informal discovery process before trial, and normally requires a non-party to provide records; it may also require personal testimony regarding the records. The general University instructions for responding to subpoenas can be found in Business and Finance Bulletin RMP-10 which is accessible at:
http://www.ucop.edu/ucophome/policies/bfb/rmp10.html

Subpoenas are not limited by the PRA exemptions; records that are confidential and non-public may still be subject to subpoena. Nor are they limited by FERPA which specifically authorizes

release of lawfully subpoenaed student records (but also requires that the institution attempt to notify the student prior to complying with the subpoena). In limited circumstances the University may file a motion in opposition to a subpoena for particularly sensitive records (i.e., confidential academic peer review records). In no case will psycho-therapeutic records be released without a court order. There are special Evidence Code provisions concerning the disclosure of Campus police officer personnel records, and any such subpoena served on a campus unit other than the UCPD should be referred to my office.

Subpoenas for records should be served upon, or addressed to, the records custodian of the department maintaining the records in question. Any person seeking to serve on the Chancellor's Office a subpoena for the records of another Campus department should be redirected to the custodian of records of that office. A subpoena for an individual to appear as a witness must be served personally upon that individual, unless another person has been authorized to accept service on his or her behalf. Subpoenas for employment records (the most frequently subpoenaed records) should be referred to Payroll Records Custodian Darrell Kelly (phone: 3-8813; e-mail: drkelly@uclink4.berkeley.edu). Subpoenas for student records should be referred to Registrar's Office Administrative Assistant Fran Verceles (phone: 2-1883; email: botver@uclink4.berkeley.edu). Subpoenas for records in the Office of the Chancellor can be accepted by either OLA or by CCRC, and immediately brought to John Cummins' attention.

Subpoenas regarding litigation in which the University is a named party should be brought to the attention of OLA and the Office of Risk Management (Leila Shockley, 3-9317). The notification should indicate the manner, date and time that the service took place. Under most circumstances, the Office of Risk Management will coordinate the processing of the response to these subpoenas.

* * * * *

Any questions regarding the scope or validity of a subpoena should be brought to Monique's or my attention. And please let me know of any records requests that have campus-wide significance, or if you have any questions about this memo.

Mike

Appendix D

PROCEDURES FOR RESPONDING TO SUBPOENAS

& Law Enforcement Requests for student Records
University of California, Berkeley – Office of the Registrar

I. INTRODUCTION

The Office of the Registrar receives requests for student records through a variety of legal means. The vast majority of these requests come in the form of *Subpoenas Duces Tecum* and *Deposition Subpoenas*—either of which may or may not require the personal appearance of the custodian of records in addition to the provision of student records. Procedures for responding to these subpoenas are addressed in sections II through X.

Other requests for student records that may be presented to the OR on occasion include *Court Orders under the USA PATRIOT Act, Grand Jury Subpoenas,* other *Law Enforcement Subpoenas, Search Warrants*, *Court Orders* or *Summons* and *Health or Safety Emergency* requests. These types of requests for student records differ in important ways from other subpoenas and are addressed in sections XI through XVI.

II. SERVICE OF A SUBPOENA

A subpoena may be served by mail, fax, or messenger. A $15.00 fee is charged per subpoena. The University must comply with subpoenas issued by officers of courts with jurisdiction over the University regardless of whether or not payment is received with the subpoena. Most subpoenas are delivered via messenger. The person delivering the subpoena will ask for a name and telephone number of the contact person in the Office of the Registrar in case someone at the notary service or attorney's office has questions. In most cases, the messenger will leave the $15.00 check with the subpoena. If not, a bill will be sent with the response to the subpoena.

III. ACCEPTANCE OF A SUBPOENA

1. There are three (3) personnel in the Student Services Office who are authorized to accept a subpoena. If presented with a subpoena, contact one the following personnel:
   - The Verifications Assistant;
   - The Special Services Supervisor; or
   - The Student Services Manager.

2. If none of the above are available, contact the Assistant Registrar.

3. Upon service of a subpoena, the authorized party should sign for it and note the date and time of receipt.

4. The Student Services Manager should be advised promptly of any attempts to serve a subpoena on the Office of the Registrar—regardless of whether or not it is accepted.

IV. RECORDS FOR WHICH THE OR IS RESPONSIBLE

1. **The Office of the Registrar is responsible for UC Berkeley scholastic records. Office of the Registrar can only** accept subpoenas for the following:
   - Academic records;
   - Student conduct records;
   - Student athletic records; and

- Student housing records.

2. Subpoenas for the following records may not be accepted **by the Office of the Registrar and should be referred to the corresponding office:**
   - UC Berkeley Extension records—UC Extension, Office of the Registrar
   - Medical records—Tang Center
   - Payroll/Personnel records—UC Human Resources
   - Police records—UC Berkeley Police Department

V. DOCUMENTING COMPLIANCE

The staff person in the Office of the Registrar designated to process subpoenas on behalf of the University of California at Berkeley must complete the cover sheet designed for guiding and recording the compliance process for each subpoena. Some of the items contained on the cover sheet include:

- Name of person whose records are requested
- Social Security Number as indicated on subpoena
- Date of birth as indicated on subpoena
- Student ID number (if available)
- Date the subpoena was received
- Due date of subpoena as indicated on subpoena
- Case number indicated on the subpoena
- Processing fee enclosed? (yes/no)
- Type and location of records
- Records requested/received from appropriate UC department (check boxes)
- Mailing address to notify the student
- Date student was notified of subpoena and USPS certified return receipt number
- Response to subpoena
- Comments

All actions taken in response to a subpoena must be recorded on the cover sheet regardless of whether or not it is specifically listed. Use the 'comments' field or the back of the form as needed.

NB: The Office of the Registrar need not make a record of disclosures under the USA PATRIOT Act, as otherwise required under FERPA.

VI. PROCESSING A SUBPOENA

1. Determine if a personal appearance is requested. If so, see section VII for procedures.

2. Determine precisely what records have been subpoenaed. If only academic records (*i.e.,* transcripts) are involved, proceed to item 3 below. If any of the other scholastic records cited in section III above are requested in addition to academic records:
   - Make photo copies of the subpoena;
   - Send the copies to the appropriate office with a memo requesting that the relevant records be sent to the Office of the Registrar;

- If the due date for compliance with the subpoena is near, telephone the other office(s) to notify them and request expedited processing.

3. Determine if the subpoenaed records exist. They may be on IDMS, Acorde, microfiche, or amongst the Confidential Files. If the records exist, request official transcripts through the proper authority. See the Student Services Manger for confidential files. If no records exist, proceed to item 5 below.

4. Determine if notification of the student/alumnus in question is required. FERPA stipulates an effort must be made to provide a student/alumnus reasonable notification that his or her records have been subpoenaed *except in the case of court orders issued under the USA PATRIOT Act, or Grand Jury or other law enforcement subpoenas that specifically indicate that the subject should not be notified.* The University of California, Berkeley interprets 'reasonable notification' to be ten (10) business days.

   Upon receipt of a court order is issued under the **USA PATRIOT Act**, inform the University Registrar and the Assistant Chancellor of Legal Affairs immediately. **Do not notify the subject(s) of the subpoena**. Proceed to item 6 below.

   If the subpoena is from a **Grand Jury** or other **law enforcement** entity and it specifically indicates that the subject(s) should not be notified, **do not notify the subject(s) of the subpoena**. Proceed to item 6 below.

5. If notification is required:
   - Determine if there is at least ten (10) business days remaining before the due date indicated on the subpoena. If there are less than ten days remaining, telephone the contact person indicated on the subpoena to inform them that an extension is required.
   - Draft a letter to the student/alumnus in question informing him/her that their records have been subpoenaed and that the University intends to comply unless a *motion to quash* (see section VI below) the subpoena is filed with the court and a copy is directed to the Office of the Registrar. All correspondence should be on UCB Office of the Registrar letterhead and signed by the Registrar. Questions should be directed to the Student Services Manager.
   - Make three (3) copies of the letter and three (3) copies of the subpoena. Send one set via first class mail to the address indicated on the subpoena or to the last known address of record for the student/alumnus in question. The second set should be sent via certified mail, return receipt. Retain the third set with the subpoena records. Be sure to record the certified mail tracking number and the date the letters were mailed on the subpoena cover sheet.
   - If no address is available, indicate this on the subpoena cover sheet.
   - In the event that there is a very short window of opportunity to notify the student/alumnus in question, attempt to contact him/her by telephone if a number is available. Written notification is still required even if the student/alumnus in question is contacted by telephone.
   - Retain the certified return receipt and any correspondence returned in the mail with the records for the subpoena.

6. Assemble requisite documents and hold them—if required—until the ten-business day notification period has elapsed. Prepare a cover letter indicating the documents enclosed and requesting payment of the $15.00 processing fee if applicable (see section X below).

   A *Declaration of the Custodian of Records* is included with most subpoenas. Simply indicate on the declaration whether or not the records are extant and affix the Registrar signature.

   If an *Affidavit* is provided in lieu of a declaration, the original Registrar signature is required instead of the signature stamp.

7. Photocopy the subpoena, cover letter and declaration/affidavit. Send the requestor a copy of the subpoena and the original cover letter and declaration/affidavit—as well as the requested records if extant. All documents should be sent via certified mail, return receipt. Retain the original subpoena and copies of the other documents with the OR subpoena record. Record the mailing date and the certified mail tracking number on the subpoena cover sheet.

VII. MOTION TO QUASH

Students/alumni who wish to prevent their records from being released must have an attorney file a *motion to quash* the subpoena with the court. As indicated in the notification letter described in section V.4 above, a copy of the motion should be directed to the Office of the Registrar in order to forestall compliance with a subpoena.

If a motion to quash a subpoena is received by the Office of the Registrar:

- Do not release the records.
- Notify the requestor in writing (via certified mail, return receipt) that the OR cannot release the records pending a ruling on the motion to quash.
- If the due date for compliance with the subpoena is near, notify the requestor by telephone, then follow-up with written notification.
- Upon written notification of a ruling on the motion, the records should be released to the requestor or filed with the OR subpoena record depending on whether or not the motion was granted.

VIII. PERSONAL APPEARANCE

If the subpoena specifies that a court appearance is required:

- Notify the Student Services Manager that a personal court appearance is required.
- Contact the office issuing the subpoena to inquire whether or not a notarized affidavit in addition to the requested records (if they exist) will suffice in lieu of a personal appearance.
- Follow the procedures outlined in section V above.
- Approximately two (2) business days prior to the appearance contact the requestor to verify that the case is still on the docket. If so, verify the exact address and time of the appearance and get directions to the courthouse. Provide the information, along with the

subpoenaed records prepared in accordance with the directions on the subpoena, to the Student Services Manager.

IX. PROCESSING FEES

There is a $15.00 processing fee for subpoenas requiring the provision of student records. An additional $35.00 fee is charged when a personal appearance is required.

Checks received—whether with subpoenas or in response to our cover letter sent with the subpoenaed records—are noted on the cover sheet upon receipt and submitted to the cashier for deposit.

USA PATRIOT Act, Grand Jury subpoenas, and other law enforcement subpoenas, search warrants, court orders and summonses are not subject to the processing fee.

X. RETENTION OF RECORDS

Subpoenas, court orders, search warrant summons, etc. and the corresponding documentation are retained for three (3) years from the response date. They may be stored off site as long as they remain reasonably accessible.

The OR need not make a record of disclosures under the USA PATRIOT Act, as otherwise required under FERPA.

XI. USA PATRIOT ACT

Court orders issued under the USA PATRIOT Act should be served in person.

Upon receipt of a court order issued under the **USA PATRIOT Act**, inform the University Registrar, the Associate Registrar for Records and Student Services and the Assistant Chancellor of Legal Affairs immediately.
Do not notify the subject(s) of the subpoena.

In consultation with the Student Services Manager, follow the steps outlined above in sections II through X—excluding section VI, item 5—to compile and provide the requested information.

The OR need not make a record of disclosures under the USA PATRIOT Act, as otherwise required under FERPA.

XII. GRAND JURY SUBPOENAS

Subpoenas issued by a Grand Jury should be served in person.

If it specifically indicates that the subject(s) should not be notified, **do not notify the subject(s) of the subpoena**. In consultation with the Student Services Manager, follow the steps outlined above in sections II through X—excluding section VI, item 5—to compile and provide the requested information.

If the subpoena does not specifically indicate that the subject(s) should not be notified, follow the steps outlined above in sections II through X to compile and provide the requested information in consultation with the Student Services Manager.

XIII. OTHER LAW ENFORCEMENT SUBPOENAS, SEARCH WARRANTS OR COURT ORDERS

On occasion, the OR may be served subpoenas, search warrants or court orders from a variety of law enforcement entities. These may be served in person, by mail or via fax. In some cases the UC Police Department may act as the liaison for the law enforcement entity.

If it is specifically stated that the subject(s) should not be notified, **do not notify the subject(s) of the subpoena**. In consultation with the Student Services Manager, follow the steps outlined above in sections II through X—excluding section VI, item 5—to compile and provide the requested information.

If it is not specifically stated that the subject(s) should not be notified, follow the steps outlined above in sections II through X to compile and provide the requested information in consultation with the Student Services Manager.

XIV. SUMMONS

A summons is a document accompanying a complaint that has been filed in court, and is treated the same as a subpoena except that: 1) there is no processing fee; and 2) all correspondence should be modified such that it refers to the 'summons' rather than the subpoena.

XV. HEALTH OR SAFETY EMERGENCIES

FERPA permits non-consensual disclosure of education records, or personally identifiable, non-directory information from education records, in connection with a health or safety emergency. This applies only to "a specific situation that presents imminent danger to a student, other students, or other members of the school community—or to a situation that requires the immediate need for information from education records in order to aver or diffuse serious threats to the safety or health of a student or other individuals."

All requests for student records in the event of health or safety emergencies are coordinated through the UC Police Department. Refer all inquiries about such matters to the UC Police Department. UCPD will assess the severity of the situation.

Upon request for student records by a UC Police official based on a health or safety emergency, notify the Student Services Manager and either the Assistant or Associate Registrar immediately. The Student Services Manager and either the Assistant or Associate Registrar will validate that the request is a health and safety emergency. A death in the student's family does not constitute a health and safety emergency.

Under the direction of the Student Services Manager and either the Assistant or Associate Registrar, promptly:

- Compile the requested records;
- Make photo copies of the requested records for the OR files;
- Note the date, time and name of UC Police official making the request;
- Provide the requested records the UC Police official; and
- Record the date, time and name of UC Police official who made the request on the first page of the OR copies of the disclosed records.

FERPA requirements for retention of disclosure records apply to health and safety emergency disclosures. See section X for retention requirements.

Should student information be needed Monday through Friday between the hours of 8:00 a.m. to 5:00 p.m., UCPD should inquire in 124 Sproul Hall.

XVI. UNUSUAL OR AMBIGUOUS SUBPOENAS

The Office of the Registrar occasionally receives an unusual subpoena or summons. Review the document carefully in consultation with the Student Services Manager. If the information requested is still unclear, the Student Services Manager will contact the Office of Legal Affairs for assistance.

Appendix E

December 3, 2001

DEANS, DIRECTORS, DEPARTMENT CHAIRS, AND ADMINISTRATIVE OFFICERS

Re: Anti-Terrorism and Student Records

On October 26, 2001, President Bush signed into law anti-terrorism legislation (P.L. 107-56). The USA PATRIOT Act of 2001allows federal law enforcement officials investigating terrorism to seek a court order requiring educational institutions to release information from student records. This new law and other incidents around the nation since September 11, 2001, have led to controversy and unfortunate rumors that law enforcement officers have been obtaining confidential student records at this campus in violation of student privacy rights (Family Educational Rights and Privacy Act, FERPA). To set the record straight, to date no student records have been sought or obtained under the new Act. In the event this does occur, we are, of course, obligated to comply with subpoenas or court orders and with FERPA in its amended form.

If served with a court order under the USA PATRIOT Act, we will follow established campus protocols for providing student records when served with a subpoena. However, in light of the concern that has been expressed on campus over this issue, I have asked that all subpoenas and court orders by law enforcement officials for student records under the PATRIOT Act be reviewed by University counsel to ensure that responses are properly framed. While the PATRIOT Act does not require notification of students when their records are subpoenaed, we will notify students unless the subpoena or court order directs otherwise for security purposes.

I share the concerns of some members of the faculty who have questioned whether such court orders might compromise academic freedom or freedom of speech. I have asked that any court orders that might raise these concerns be brought to my personal attention prior to response. I welcome advice from the Academic Senate on these matters.

The new law does not alter or negate in any way the University's long standing welcome to and protection of students, staff and faculty of all backgrounds and nationalities. The tragic events of September 11 have not changed the environment at UC Berkeley for international students, and have not lessened our commitment to diversity of views, free speech and civil debate. The campus remains fully committed to protecting student privacy within the boundaries established by law.

The new law also does not alter the basic campus procedures and delegations of authority for responding to student records requests. University officials responsible for student records should be familiar with those procedures and protections. However, I ask that you take this opportunity to remind your staff about FERPA and University policies regarding the appropriate disclosure of information from student records. The policies can be found in electronic form at: http://uga.berkeley.edu/uga/disclosure.stm.

If you or your faculty or staff should receive a court order or subpoena for student records, please refer the server of the order/subpoena to Registrar Susanna Castillo-Robson, 120 Sproul Hall (642-2261). Questions about FERPA or campus procedures for responding to requests for student records can be directed to her as well. Any law enforcement requests (whether subpoenas, warrants, or other like requests) also should be brought to the attention of Assistant Chancellor Michael Smith (642-7122).

Robert M. Berdahl
Chancellor

UNITED STATES DEPARTMENT OF EDUCATION

WASHINGTON, D.C. 20202

Recent Amendments to Family Educational Rights and Privacy Act Relating to Anti-Terrorism Activities

April 12, 2002

Dear Colleague:

The purpose of this guidance is to provide you with an overview of recent changes made by Congress to the Family Educational Rights and Privacy Act (FERPA) in response to the September 11th terrorist attacks on the United States. In so doing, we also will provide an overview of the relevant provisions of current law. The changes to FERPA became effective on October 26, 2001, when the President signed into law the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001." (Public Law 107-56; 115 Stat. 272.) Section 507 of the USA PATRIOT ACT amends FERPA, and is attached for your convenience at the end of this letter.

Overview of FERPA

FERPA is a federal law that applies to educational agencies and institutions that receive federal funds under any program administered by the Secretary of Education. 20 U.S.C. § 1232g; 34 C.F.R. Part 99. Generally, FERPA prohibits the funding of an educational agency or institution that has a policy or practice of disclosing a student's "education record" (or personally identifiable information contained therein) without the consent of the parent. When a student turns 18 years old or attends a postsecondary institution at any age, the rights under FERPA transfer from the parent to the student ("eligible student").

FERPA defines "education records" as "those records, files, documents and other materials which –

(i) contain information directly related to a student; and
(ii) are maintained by an educational agency or institution or by a person acting for such agency or institution."

20 U.S.C. § 1232g(a)(4)(A)(i) and (ii).

FERPA generally requires prior written consent from the parent or eligible student before an educational agency or institution may disclose personally identifiable information from education records to a third party. However, the law contains 16 exceptions to this general rule. Pertinent exceptions that allow release of personally identifiable information without prior written consent are discussed below.

Ex Parte Orders

Significantly, the recent amendment to FERPA permits educational agencies and institutions to disclose – without the consent or knowledge of the student or parent – personally identifiable information from the student's education records to the Attorney General of the United States or to his designee in response to an *ex parte* order in connection with the investigation or prosecution of terrorism crimes specified in sections 2332b(g)(5)(B) and 2331 of title 18, U.S. Code.[2] An *ex parte* order is an order issued by a court of competent jurisdiction without notice to an adverse party.

In addition to allowing disclosure without prior written consent or prior notification, this provision amends FERPA's record keeping requirements (20 U.S.C. § 1232g(b)(4); 34 C.F.R. § 99.32). As a result, FERPA, as amended, does not require a school official to record a disclosure of information from a student's education record when the school makes that disclosure pursuant to an *ex parte* order. Further, an educational agency or institution that, in good faith, produces information from education records in compliance with an *ex parte* order issued under the amendment "shall not be liable to any person for that production."

A copy of the new statutory language follows this guidance. The Department will be working with the Department of Justice in the implementation of this new provision. In addition to this guidance, we will be amending and updating the FERPA regulations to include this new exception to the written consent requirement. You should address any questions you have on the new amendment to FERPA@ED.Gov.

Lawfully Issued Subpoenas and Court Orders

FERPA permits educational agencies and institutions to disclose, without consent, information from a student's education records in order to comply with a "lawfully issued subpoena or court order" in three contexts. 20 U.S.C. § 1232g(b)(1)(J)(i) and (ii), (b)(2)(B); 34 C.F.R. § 99.31(a)(9). These three contexts are:

1. Grand Jury Subpoenas – Educational agencies and institutions may disclose education records to the entity or persons designated in a Federal grand jury subpoena. In addition, the court may order the institution not to disclose to anyone the existence or contents of the subpoena or the institution's response. If the court so orders, then neither the prior notification requirements of § 99.31(a)(9) nor the recordation requirements at 34 C.F.R. § 99.32 would apply.

2. Law Enforcement Subpoenas – Educational agencies and institutions may disclose education records to the entity or persons designated in any other subpoena issued for a law enforcement purpose. As with Federal grand jury subpoenas, the issuing court or agency may, for good cause shown, order the institution not to disclose to anyone the

[2] These statutes define Federal crimes of terrorism as offenses calculated to influence the conduct of government such as destruction of aircraft, assassination, arson, hostage taking, destruction of communications lines or national defense premises, and use of weapons of mass destruction.

existence or contents of the subpoena or the institution's response**.** In the case of an agency subpoena, the educational institution has the option of requesting a copy of the good cause determination. Also, if a court or an agency issues such an order, then the notification requirements of § 99.31(a)(9) do not apply, nor would the recordation requirements at 34 C.F.R. § 99.32 apply to the disclosure of education records issued pursuant to the law enforcement subpoena.

3. All other Subpoenas – In contrast to the exception to the notification and record keeping requirements described above, educational agencies or institutions may disclose information pursuant to any other court order or lawfully issued subpoena only if the school makes a reasonable effort to notify the parent or eligible student of the order or subpoena in advance of compliance, so that the parent or eligible student may seek protective action. Additionally, schools must comply with FERPA's record keeping requirements under 34 C.F.R. § 99.32 when disclosing information pursuant to a standard court order or subpoena.

Health or Safety Emergency

FERPA permits non-consensual disclosure of education records, or personally identifiable, non-directory information from education records, in connection with a health or safety emergency under § 99.31(a)(10) and § 99.36 of the FERPA regulations. In particular, § 99.36(a) and (c) provide that educational agencies and institutions may disclose information from an education record "to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals" and that the exception will be "strictly construed." Congress' intent that the applicability of this exception be limited is reflected in the *Joint Statement in Explanation of Buckley/Pell Amendment*, 120 Cong. Rec. S21489 (Dec. 13, 1974).

Accordingly, the Department consistently has limited the health and safety exception to a specific situation that presents imminent danger to a student, other students, or other members of the school community – or to a situation that requires the immediate need for information from education records in order to avert or diffuse serious threats to the safety or health of a student or other individuals. For example, the health or safety exception would apply to nonconsensual disclosures to appropriate persons in the case of a smallpox, anthrax or other bioterrorism attack. This exception also would apply to nonconsensual disclosures to appropriate persons in the case of another terrorist attack such as the September 11 attack. However, any release must be narrowly tailored considering the immediacy, magnitude, and specificity of information concerning the emergency. As the legislative history indicates, this exception is temporally limited to the period of the emergency and generally will not allow for a blanket release of personally identifiable information from a student's education records.

Under the health and safety exception school officials may share relevant information with "appropriate parties," that is, those parties whose knowledge of the information is necessary to provide immediate protection of the health and safety of the student or other individuals. 20 U.S.C. § 1232g(b)(1)(I); 34 C.F.R. § 99.36(a). Typically, law enforcement officials, public health officials, and trained medical personnel are the types of parties to whom information may

be disclosed under this FERPA exception. FERPA's record keeping requirements (§ 99.32) apply to disclosures made pursuant to the health or safety exception.

The educational agency or institution has the responsibility to make the initial determination of whether a disclosure is necessary to protect the health or safety of the student or other individuals. However, the Department is available to work with institutions to assist them in making such decisions in order to ensure that the disclosure comes within the exception to FERPA's requirement of prior written consent.

In short, the health or safety exception will permit the disclosure of personally identifiable information from a student's education record without the written consent of the student in the case of an immediate threat to the health or safety of students or other individuals. Of course, a school official, based on his or her own observations, may notify law enforcement officials of suspicious activity or behavior. Nothing in FERPA prohibits a school official from disclosing to federal, State, or local law enforcement authorities information that is based on that official's personal knowledge or observation and not from an education record.

Law Enforcement Unit Records

Under FERPA, schools may disclose information from "law enforcement unit records" to anyone – including federal, State, or local law enforcement authorities – without the consent of the parent or eligible student. FERPA specifically exempts from the definition of "education records" – and thereby from the privacy restrictions of FERPA – records that a law enforcement unit of a school district or postsecondary institution creates and maintains for a law enforcement purpose. A "law enforcement unit" is an individual, office, department, division, or other component of a school district or postsecondary institution – such as a unit of commissioned officers or noncommissioned security guards – that is officially authorized or designated by the school district or institution to: (1) enforce any federal, State, or local law; or (2) maintain the physical security and safety of the school. See 34 C.F.R. § 99.8.

FERPA narrowly defines a law enforcement record as a record that is: (i) created by the law enforcement unit; (ii) created for a law enforcement purpose; and (iii) maintained by the law enforcement unit. 34 C.F.R. § 99.8(b). While other components of an educational institution generally can disclose, without student consent, student education records to school law enforcement units (under FERPA's exception for school officials with legitimate educational interests), these records are not thereby converted into law enforcement unit records because the records were not created by the law enforcement unit. Thus, a law enforcement unit cannot disclose, without student consent, information obtained from education records maintained by other components of an educational institution.

Directory Information

FERPA's regulations define "directory information" as information contained in an education record of a student "that would not generally be considered harmful or an invasion of privacy." 34 C.F.R. § 99.3. Specifically, "directory information" includes, but is not limited to the student's name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status (e.g., undergraduate or graduate, full-time or part-time), participation in officially recognized activities or sports, weight and height of members of athletic teams, degrees, honors and awards received, and the most recent educational agency or institution attended. Id. A school may disclose "directory information" from the education records without prior consent only after giving notice to the student of its directory information policy, and providing parents and eligible students with an opportunity to opt out of having their "directory information" disclosed. See 34 C.F.R. § 99.37.

Under FERPA, a school may not comply with a request for "directory information" that is linked to other non-directory information. For instance, a school cannot disclose "directory information" on students of a certain race, gender, or national origin. However, the school could disclose "directory information" on *all* students (who have not opted out) to law enforcement authorities who may be requesting "directory information."

Disclosures to the Immigration and Naturalization Service (INS)

The Immigration and Naturalization Service (INS) requires foreign students attending an educational institution under an F-1 visa to sign the Form I-20. The Form I-20 contains a consent provision allowing for the disclosure of information to INS. The consent provision states that, "I authorize the named school to release any information from my records which is needed by the INS pursuant to 8 C.F.R. 214.3(g) to determine my nonimmigrant status." This consent is sufficiently broad to permit an educational institution to release personally identifiable information of a student who has signed a Form I-20 to the INS for the purpose of allowing the INS to determine the student's nonimmigrant status. Students that have an M-1 or J-1 visa have signed similar consents and education records on these students may also be disclosed to the INS.

Finally, we anticipate there may be a need for additional guidance in the future on other INS disclosure issues.

For additional guidance on these or other provisions of FERPA contact the Family Policy Compliance Office at the following address and telephone number:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202-4605
(202) 260-3887 – Telephone
(202) 260-9001 – Fax

Additionally, schools officials may contact the Family Policy Compliance Office by e-mail for quick, informal responses to routine questions about FERPA. That address is: FERPA@ED.Gov. The Web site address is: www.ed.gov/offices/OM/fpco.

Sincerely,

/s/

LeRoy S. Rooker
Director
Family Policy Compliance Office

Appendix G

Policies and Protocols
Regarding the Disclosure of Information from Academic Personnel Records

Policies and protocols regarding the disclosure of information from academic personnel files are delineated in UC Business and Finance Bulletin RMP-8: Legal requirements on Privacy of and Access to Information Education Rights and Code, Public Records Act; UC Business and Finance Bulletin RMP –7: Privacy of and Access to Information Responsibilities and the UC Business and Finance Bulletin RMP-9, Guidelines for Access to University Personnel Records by Governmental Agencies Correspondence.

Berkeley campus practices are consistent with those outlined in RMP-8, RMP-7 and RMP-9.

A substantial amount of the information from RMP-8 is embedded in other campus policies, such as:

- Academic Personnel Manual 160 – access to academic records;
- Personnel Policies for Staff Members (PPSM-80) – staff personnel records
- UC Contract & Grant Manual, Chapter 17 – access to research records

Several departments on campus publish specific guidelines for responding to requests for PRA and IPA documents, including:

- The Sponsored Projects Office http://www.spo.berkeley.edu/Procedures/records.html
- The Information Systems & Technology Division http://socrates.berkeley.edu:2002/pols.html
- The Office of the Registrar http://registrar.berkeley.edu/GeneralInfo/ferpa.html

All PRA-IPA requests must be specific in nature and in writing. A response to the requester is required within 10 days indicating the campus willingness to provide the data. Currently, units charge between 10 cents and 25 cents per page for copying documents requested.

Appendix H

UC Berkeley Library January 12, 2003

What to do if I am approached by the FBI or the Police

If a law enforcement official approaches you requesting information from Library records refer all inquiries to Library Administration, 245 Doe.

TWO SCENARIOS

1) If they present a **SUBPOENA**, direct either the person or the paper to your supervisor or department head: (insert name of supervisor/dept head) who will in turn direct it immediately to Library Administration, 245 Doe.

If your supervisor or department head is not in the office, direct the person or take the subpoena to Library Administration, 245 Doe. If the subpoena is delivered during evening or weekend hours, place the subpoena in the department head's mailbox and **note the day and time of receipt on the back of subpoena**. It is important to realize that subpoenas do not demand immediate action.

2) If they present a **WARRANT,** do not interfere with their search or seizure. Inform your direct supervisor. Your direct supervisor (or you, if there is no supervisor) should call your emergency contact person _____ as soon as possible.

Call the UCB Police Department at 642-3333. They will ensure all rules of the warrant are followed.

When the law enforcement people leave with library property, they will leave a receipt concerning the items removed. Please pass this on to your direct supervisor.

What happens next?
Library Administration will then refer the server of the order/subpoena to university counsel. Any law enforcement requests (whether subpoenas, warrants, or other like requests) will be brought to the attention of Assistant Chancellor Michael Smith (642-7122).

Appendix I

Proposed Modifications to Protocol for Non-Consensual Disclosure of Electronic Information Contained in the Electronic Communications Policy In Light of the USA PATRIOT Act[3]

Inspection and Review

In the event of any request for disclosure, inspection or monitoring of the contents of a holder's electronic records when required by and consistent with law (Section IV.B. Access without Consent)[4], the ECP requires advance written authorization by the Vice Chancellor for Research (Section IV.B.1). Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

In contrast, if an inspection is requested by means of a USA PATRIOT ACT subpoena, the Vice Chancellor for Research should only be notified that the subpoena was received without revealing the identity of the individual whose electronic communications records are requested.

Emergency Circumstances

In emergency circumstances (IV.B.2), the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay (Section IV.B.1, Authorization). Again, if the emergency is pursuant to the USA PATRIOT Act, the Vice Chancellor for Research shall only be notified as stated above.

The ECP specifies that the affected individual should be notified at the earliest possible opportunity that is lawful and consistent with other University policy. This requirement, however, shall be suspended if inspection is requested by means of a USA PATRIOT ACT request.

UCOP Reporting Requirements

The campus must submit an annual report to the Office of the President, summarizing instances of non-consensual access to electronic communications records. Any USA PATRIOT ACT requests shall be included in this report without revealing any personally identifiable information.

[3] USA PATRIOT Act changes underlined.

[4] http://www.ucop.edu/ucophome/policies/ec/html/ecppolicy_sectionIV_pivacyandconfidentiality.htm#SectionIV-B

The ECP specifies that advice of counsel must always be sought prior to any action taken under Sections IV.B.1, Authorization, and IV.B.2, Emergency Circumstances, involving electronic communications (a) stored on equipment not owned or housed by the University, or (b) whose content is protected under the federal Family Educational Rights and Privacy Act of 1974. The Office of the General Counsel (OGC) has advised that this requirement shall remain for requests made under the USA PATRIOT Act, as OGC has defined University counsel to be part of the "need to know" team in complying with the request.

The ECP requires that a recourse mechanism must be provided to individuals who believe that actions taken by employees or agents of the University were in violation of this Policy. This section is suspended in the event of a USA PATRIOT ACT request since the University "shall not be liable to any person" for good faith disclosure of records in response to such a court order.

Costs for Retrieval of Records

Efforts to comply with USA PATRIOT ACT requests for electronic records stored on central systems (UCLink or Socrates) backup media should expect to encounter significant expense. CCS retains a full month of daily backup tapes and a year of monthly backup tapes. These tapes will only contain what was in an individual's mail store at the time the backup was run. They will not contain any email messages that may have been downloaded to the user's workstation or deleted between backups.

Most of these tapes are stored off-site. Offices should note that it could take between 80 and 120 hours of work to recover up to a year's worth of an individual's email records. The established recharge labor rate for such work is $72 per hour.

Appendix J

Draft Protocols for Responding to Health and Safety Emergencies

Overview and Definition

The Family Educational Rights and Privacy Act (FERPA) governs the disclosure of information from student records and access to these records. FERPA and University policy generally prohibit the disclosure of personally identifiable, non-directory information (also referred to, on the Berkeley campus, as confidential information) about students to third parties without first obtaining prior written consent from the applicable student. There are, however, certain exceptions to this general rule. One pertinent exception that allows release of confidential information without prior written consent is the Health and Safety exception.

FERPA permits educational institutions to disclose confidential information from student records "to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals." The Health and Safety exception is significantly limited as defined below:

- The exception applies to a specific situation that presents imminent danger to a student or others of the UC Berkeley community or to a situation that requires the immediate need for information from student records in order to avert or diffuse serious threats to the safety or health of a student or other individuals.

- Disclosure must be narrowly tailored considering the immediacy, magnitude, and specificity of information concerning the emergency.

- The Health and Safety exception is temporally limited to the period of the emergency.

Protocols

As educational institutions are responsible for making the initial determination of whether a disclosure is necessary to protect the health or safety of the student or other individuals, the Berkeley campus has established the following protocols for requesting student information relating to health and safety emergencies.

1. When confronted with a possible Health and Safety emergency, contact the UC Police Department (UCPD) immediately at 642-6760. The nature and urgency of the emergency should be explained to the responding UCPD officer, as well as the need to access student information. Immediate threats to public safety should be reported to UCPD by dialing 9-1-1 or 642-1133.

2. The UCPD should assess the severity of the situation. If UCPD determines the situation to be a Health and Safety emergency, as defined above, and requires student information, UCPD should contact the Office of the Registrar (OR) at:

124 Sproul Hall (8:00 AM to 5:00 PM, Monday through Friday)

3. OR should assess UCPD's request for student information and determine whether disclosure would be permissible under FERPA and University policy. If so, then OR should provide UCPD with only enough relevant information from the student record to handle the health and safety emergency.

4. If the Health and Safety emergency occurs at any time other than Monday through Friday, 8:00 AM to 5:00 PM, or on an academic/administrative holiday, the UCPD should contact the on-call UCPD Command Officer, who will assess the urgency of the situation and, if necessary, initiate contact with the appropriate campus administrator to obtain access to the student information.

5. The office that maintains the student record(s) must keep a record of the request for access to and disclosure of confidential information from those records.

6. The UCPD, upon obtaining confidential information from student records, shall use the information only for the purpose for which the disclosure was made (that is, the health and safety emergency), and shall not improperly redisclose the information to any other party without the prior consent of the student.

Appendix K

IPA Coordinator & PRA practices

Public Record Act Models at UCSF and UCLA

UCSF: The IPA Coordinator is the Chief Campus Counsel, who has an Associate Campus Counsel, and a high level administrator (Principal Analyst), reporting to her. The Principal Analyst handles the IPA/PRA requests. The Chief and Associate Campus Counsels call OGC on complex requests, but their office is where all campus units come to, when an IPA/PRA request arrives.

The Principal Analyst and is in charge of the Chancellor's Office Central Records Management. (CCRC) The Principal Analyst is the key contact on campus for all PRA requests and is responsible for the process of responding.

UCSF process of response:

1) CCRC logs the receipt of the PRA request
2) The CCRC Principal Analyst sends the letter of response (with in 10 day timeframe) to requestor
3) The CCRC Principal Analyst contacts the chief of staff in each Vice Chancellor's office for help with the information requested.
4) The chief of staff in the VC's office then delegates the appropriate person in their unit to work on collecting the data. The data is collected and sent back to CCRC.
5) The Principal Analyst compiles the data and asks for help from Campus Counsel on items to include (or redact) or asks for help from Office of General Counsel.
6) The Principal Analyst sends out the final copy to the requestor at a cost of 10 cents a page.

UCLA: The IPA Coordinator is the Director of Business and Finance, who oversees all records management CCRC. The IPA Coordinator has a top administrator, a Senior Administrative Analyst in CCRC, who is the key contact on UCLA campus for all PRA requests and is responsible for the process of responding.

UCLA process of response:

1) CCRC logs the receipt of the PRA request
2) The Senior Administrative Analyst sends the letter of response (with in 10 day timeframe) to requestor
3) The Senior Administrative contacts the chief of staff in each Vice Chancellor's office for help with the information requested.
4) The chief of staff in the VC's office then delegates the appropriate person in their unit to work on collecting the data. The data is collected and sent back to CCRC.
5) The Senior Administrative Analyst compiles the data and asks for help from her campus counsel on items to include (or redact) or asks for help from Office of General Counsel.

6) The Senior Administrative Analyst sends out the final copy to the requestor at a cost of 10 cents a page.

UCLA PRA "how to handle" information on their campus web site:
http://www.finance.ucla.edu/Records/public_records_faq.htm

IPA & PRA Background on UC Berkeley Campus:

The Principal Analyst, VP Office of Academic Affairs and Faculty Welfare, researched the Berkeley campus and other UC campus models for handling Public Records Requests. The Office of General Counsel (OGC) offered the following suggestions as to how campuses might structure their Information Practices Coordinator position and how to handle PRA requests:

> The campus Information Practices Act Coordinator is appointed by the Chancellor, as required by RMP-7. The recommended standard model for PRA requests would be for a campus to appoint a high level administrator to be the central campus coordinator for all IPA and PRA requests. This person would have direct access to their campus IPA Coordinator who would be either their campus general counsel or a top administrator in their campus business administration (financial records) area. Also, OGC recommends the campus IPA appointee be a long-term appointee, to establish credibility on their campus as the authority on records requests, and to help keep the campus & OGC running smoothly. With the climate in the business community becoming increasingly litigious, it is imperative that each campus has their IPA Coordinator clearly designated and empowered to handle these complex requests. OGC specified that no campus appoints an academic as their campus IPA coordinator.
>
> Historically on the UC Berkeley campus, Chancellor Tien appointed the first IPA Coordinator (the Academic Compliance Officer), who retired in Fiscal Year 1993-1994. The next campus appointed IPA Coordinator was came on board in 2000. Since the campus IPA Coordinator's departure in June 2002, the Chancellor has not appointed another campus IPA Coordinator.