University
of
California

Information Resources
& Communications
http://www.ucop.edu/irc/

Published by IR&C as
a service to staff at the
Office of the President

Spring 2000

In This Issue

inside INFO

Public Key Infrastructure

Planning for the Future

What could be more efficient than Internet-based transactions? No cumbersome paper forms, no waiting for approvals, no time wasted providing duplicate information. What could be more alarming than Internet-based transactions? No guarantee that a person is who they say they are, no confirmation that documents have not been altered, no guarantee that personal information is protected from snooping.

If the Internet is to deliver its full promise of efficiency, solutions must be found to the problems of authentication (you are who you say you are), document integrity (the document you signed has not been altered), and confidentiality (no one can access sensitive data without appropriate approvals). UC is at the forefront of national efforts to solve these problems by implementing a technology called Public Key Infrastructure (PKI)—favored by experts in government and industry as the most feasible way to address these problems.

Universitywide working groups have developed the systems architecture for an integrated University-wide PKI, draft policies have been prepared by UCOP, and a vendor has been selected to provide PKI technology across the University. A PKI pilot program will soon be launched at each campus in the next few months. In the meanwhile, other institutions are learning from the work of UC individuals.

continued on page 3

Streamlining & Updating

Retirement & Benefits Systems

IR&C and HR/Benefits are collaborating on a major systems re-engineering project that will eliminate paperwork, speed response time, and provide employees direct access to information about their own retirement and investment accounts. The project, which involves reengineering both business processes and technology, is part of a strategic plan known as the Employee Systems Initiative (ESI). The ESI was developed by the Employee Systems Task Force in 1997.

The project will integrate direct employee access to Web-based systems with electronic imaging of permanent records. Web interfaces will replace forms as the means by which employees create their own records, access information about their accounts, and make requests for certain services. Electronic imaging will create digital files that display images of physical documents, including those bearing signatures, and can be retrieved and displayed by computers. Use of these technologies reduces the need for paper files and for many data entry tasks, enabling HR/Benefits to respond to the needs of the user community of employees faster and more effectively than ever before. New processes using these techniques are now available in the following areas:

Disability - This was the first automated workflow project to employ both electronic imaging and work queues to distribute work. The disability

continued on page 2

HR Benefits

continued from page 1

unit's work involves sending out requests for information and then assembling the returned responses, which used to be done by sending paper forms, assembling them on a single desk, and initiating an administrative action when the information was complete. The new system uses electronic interfaces to collect information, which is sent to "rendezvous queues" that electronically trigger administrative action when certain pieces of information arrive. Similarly, "call-up queues" trigger follow-up action when an expected response does not come within the anticipated time frame.

Loans - The process for application, approval, and funding of 403(b) loans has been completely revamped. Loan application forms were replaced by an interactive voice response (IVR) system. The workflow system automatically pushes each IVR-generated application through the approval, auditing, and commitment stages. The imaging system automatically generates and captures promissory notes, which are sent to the employee for physical signature. Upon receipt of the signed promissory notes, the workflow system initiates the funding operation and check generation.

Retirement - Another workflow/imaging project addresses the retirement process. Initiated by a web-based system, the new workflow system computes retirement options and generates all the necessary documentation to provide the employee with information about his or her retirement balances and options. Once the employee returns the signed document, it is imaged and the workflow system interfaces with the Annuitant System to begin retirement payments and with the Insurance System to continue Health Benefits.

Refunds - An IVR front-end and an automatic check generation process have replaced paper forms for employee requests for Voluntary Disbursements (refunds) from the retirement system. Checking eligibility for a refund, which used to be a manual process, is now done automatically at the time the employee requests the refund.

Event Tracking - All of the new processes log significant events to the Event Tracking System. For example, receipt of correspondence or a loan application from an employee and the mailing out of a promissory note are all recorded in the Event Tracking system. Benefits personnel can make inquiries of the system to ascertain the status of any process for a particular employee. The Event Tracking System interfaces with the imaging system in such a way that it will not only show that correspondence or the loan application was received but also provide a direct link to the image of that document.

These are only the first of many joint IR&C and HR/Benefits workflow re-engineering projects.

Bruce James

Digital California Project to Bring Advanced Internet to K-12

California will invest $31 million in FY 2000-01 to bring high speed advanced networking closer to K-12 schools through the Digital California Project (DCP), a CENIC (see p. 8) initiative funded through UC.

IR&C staff helped CENIC leadership develop the project plan and worked with representatives of CENIC, and UC's Budget Office and Office of State Governmental Relatins to refine the plan.

DCP will use CENIC's advanced services Internet (CalREN-2) to facilitate collaboration among K-12, higher education, and new on-line educational resources. The DCP will extend CalREN-2 to provide a total of up to 200 high speed connection points for K-12 schools in all of California's 58 counties. School districts will not be charged for using these services but will have to develop their own local network infrastructure, link to one of the 200 connection points, and provide local support services. The connections will allow access to the general Internet and resources at UC, CSU, Stanford, Caltech and USC. Work will begin in August with the first K-12 connections next Spring.

David Wasley

Public Key Infrastructure

continued from page 1

What is PKI?

PKI was developed to address a wide range of administrative and business processes that require: proof of the identity of participants in a transaction, proof that the contents of communications have not been tampered with, and protection of sensitive or restricted data.

It is based on digital certificates that verify the identity of individuals and the integrity of documents. The U.S. Government has proposed that digital certificates be accepted for many purposes that now require physical signatures or physical controls on the handling of data and records. California has also enacted legislation to recognize as legal "digital signatures" that are created by use of PKI.

How PKI works

PKI uses encryption technology to create and verify digital documents that are very difficult to alter or forge. "Certificate authorities" issue digital credentials in a process that resembles the way passports or student ID cards are issued: an individual proves his or her identity to the issuing authority and receives a digital credential or "certificate," a small file containing identifying information and a pair of encryption keys. The encryption keys enable the holder of the certificate to prove his or her identity both to gain access to restricted resources and to create digital documents that cannot be altered. The issuing authority maintains repositories of the credentials it issues for use by anyone who wishes to confirm that a digital certificate is genuine.

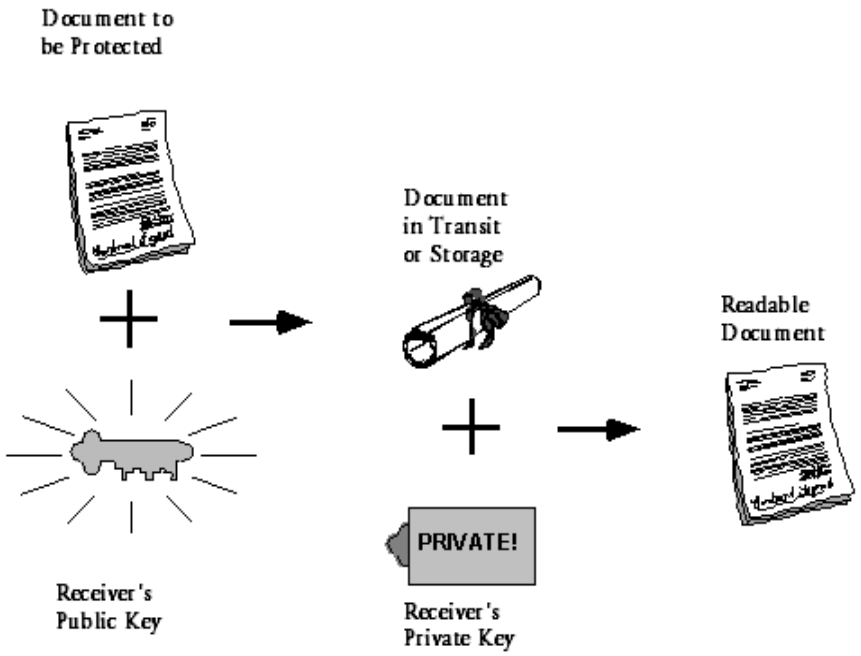
PKI overcomes the limits of passwords as the primary tool for protecting sensitive resources. Passwords were adopted as the standard in the early days of computing, when limited groups of technical employees used dedicated terminals to gain access to a single computer system. There was little risk that the passwords would be intercepted in transit from the terminal to the mainframe, and few people had access to computers powerful enough to guess another's password. Today, individual PCs gain access to hundreds of computers via the Internet, often sending unencrypted passwords to "host" computers for a wide range of purposes. Moreover, with easily available software and enough time, desktop PCs can guess almost any host computer password. Widely publicized cases have demonstrated the damage that can result when private or confidential information such as credit card and Social Security numbers becomes accessible to unauthorized parties.

The Uses of PKI

PKI provides a convenient and robust method of controlling access to the variety of restricted systems and other online resources used by members of the University community. Instead of having to remember and type many different passwords, individuals will use a digital certificate and a private key that are either (1) stored on a computer's hard drive and accessible only to a person who both has physical access to the computer and knows the password; or (2) stored on a portable "smart card" similar to an ATM card. The same technology can provide security at various levels for UC computer resources that range from digital library reserves to online databases of personal information such as retirement system balances and student grades.

PKI also provides a means of enabling

continued on page 4



A sender wishing to secure a document during transit or storage encrypts it with the Public Key of the Receiver or potential reader. The document can be recovered only by use of the intended reader's Private Key.

Public Key Infrastructure

continued from page 3

"signatures" on digital documents. These can be archived with the digital certificate as evidence that the documents have not been altered after they were "signed." Indeed, digital documents authenticated with digital certificates are more difficult to forge than paper forms and ink signatures. California legislation enacted last year permits legally binding contracts to be signed digitally using PKI technology. UC's initial PKI program will not include digital signature capability, but it will lay the groundwork for new business processes that can treat digitally signed documents with the same confidence now given to manually signed documents.

Implementation

UC will implement PKI Universitywide with pilot projects at every location. The Universitywide PKI effort will allow the University to speak with one voice when developing agreements for use of its digital credentials to interact with outside agencies and organizations, whether public or private. For example, procedures developed to allow use of PKI technology in conjunction with Federal agencies will need be developed only once.

The Universitywide implementation will preempt local implementations that could require costly remediation in the future. Although individual departments, schools and colleges are beginning to experiment with and use PKI, such individual implementations will not work well together if not specifically structured to do so. Multiple implementations of PKI also risk creating a situation in which digital credentials issued by one PKI are not recognized as valid by another. In such a scenario, University records would become inaccessible to authorized individuals, and business transactions might be undertaken in ways that create unnecessary University liability. Finally, the Universitywide deployment of PKI, accompanied by appropriate policy, will avoid misrepresentation of the University's name in digital credentials that might otherwise be issued independently by departments.

University PKI Plan

Centralized Universitywide funding, in addition to an investment of staff resources at the campuses and UCOP, will give each University faculty, staff member, and student access to digital credentials. Once University digital credentials are widely available, newly designed systems will be able to accept certificates rather than or as well as passwords. Then the University can begin experiments with "secure" email, approaches for using PKI for encrypting University files, and the implementation of digital signatures.

Public Key Infrastructure technology is properly viewed as an additional layer of University investment in the Internet and Internet technologies. While not part of today's common vocabulary, PKI and Digital Certificates are rapidly being integrated into the next wave of Internet applications and are critical to its growth. PKI offers the foundation for greatly improved security of confidential information stored in databases and sent from personal computers to databases over the Internet. It can support secure, legally binding digital business transactions and participation in electronic commerce with legally signed documents. PKI also provides a foundation for ensuring the authenticity of official University records (which are increasingly created and stored in digital form), of email senders, and of the content of email messages.

Jim Dolgonas

Eyes on the Web

See Automated Services for UC Employees on the Bencom web site
http://www.ucop.edu/bencom/news/ucfy.html

UC For Yourself is located at
http://ucfy.ucop.edu/NetDynamics/NetDynamics40/ndconfig.nd/ucopNDBase/pgUcopLogin

UCLA has a Welcome to UCOP Employees page on the web. Go to
http://www.payroll.ucla.edu/ucop/ucop.htm

The California Digital Library provides a News and Developments page to keep you up to date
http://www.cdlib.org/news/

Technology Behind the CDL

Twice a year, in January and July, the California Digital Library unveils major new features, offering a continuously expanding array of digital resources to the University. Conceived and planned by University Librarian Richard Lucier and his senior staff in collaboration with librarians and faculty at every campus, new features provide services identified as high-priority for research and teaching.

Behind each new "release"–the moment when a new feature becomes operational– is a months-long process of technology planning, programming, and database management. One to two months before its public introduction, a "mirror" copy of a new application is installed on a machine separate from CDL's servers for testing by beta users on every campus. The beta users experiment to determine whether the application works as intended, confirm that all components are integrated, and identify problems for the CDL-T programmers to fix. On the public release date, the production copy of the application becomes available to the University community on a CDL server.

Millennium Releases

Major new features offered in January were Searchlight, which helps users locate material, and Phase II of Request, , which allows users to obtain materials held at libraries on other campuses. Phase I (released in January 1999) allowed interlibrary loan (ILL) of monographs, while Phase II allows ILL of articles, videos, and other forms of materials. Coming in July is "My Library," a tool for customizing a personal library page, and a CDL directory of resources on UC campuses.

Searchlight allows users to search for keywords across either the social science/humanities or the science/technology portions of the CDL's collection of databases and retrieve information on the number of "hits" each database yields. For many of these information resources, the Searchlight results page provides a live link to the relevant findings. Where direct links are not available, the search results still help the user decide which databases to target for future searches. Previously, users had to search one database at a time without advance knowledge of the likely number of resources to be found.

The Request feature allows users to request that a paper article or monograph available on another campus be delivered to the user's home library. If the material is already on loan at the home campus, Request will obtain the material from another UC campus. Additionally Request allows users to ask for document delivery of materials owned by the campus library (not all campuses provide document delivery). To initiate a Request the user searches one or more of the CDL hosted databases, identifies the desired materials, and clicks on the Request button. After verifying the user's status, the Request service sends this ILL request directly to the lending institution to be filled. This streamlines the traditional ILL process by bypassing the home campus ILL unit's traditional activities of manual verification and transmission of ILL requests.

Search

For Searchlight, which built on work first done at UC San Diego, the challenge was to develop a search strategy that could identify and interpret information stored in different fields and formats in a wide variety of databases, some housed at UCOP, some on campuses, and some at publishers' external sites. Databases hosted by CDL conform to the Z39.50 search format and can be searched by the same set of programming instructions. However, many of the databases included in the CDL are hosted at external vendor sites for which only Web tools are available, challenging CDL programmers to develop strategies to minimize irrelevant results.

Authentication

The Request feature posed a different challenge: how to ensure that a user who makes a request at one campus for material held at another is in fact entitled to do so. Within individual campuses, this authentication process is managed through the familiar device of a library card, which is related to a user information database. Traditionally, intercampus borrowing was managed by library-to-library interactions, in which the receiving library lends the material to its user and accepts responsibility for returning the material to the sending library.

With the increasing availability of electronic texts and photocopies of individual articles, the need to guarantee return of materials has declined and user-to-remote-library interactions are feasible if the sending library is sure the user is an authorized borrower. The initial solution was for the Request server to check a combined patron database maintained by IR&C for all campuses except UCB. Real time patron checks are done on the UCB library patron database. By the end of this year, however, user requests will be automatically referred to and cleared through campus-maintained databases for 8 of the 9 campuses. The Request server is also

continued on page 8

Patrick Collins Joins Information Management

On May 1st Patrick Collins joined IR&C as the newly appointed Director of Information Management. Patrick spent his first days here getting to know his staff and meeting with users of corporate systems. Patrick's short term goals are to fill the vacant positions in IM and begin to offer training on the data warehouse components that are already in place.

Information Management will maintain support for FOCUS and all of the current production reports while facilitating the migration of corporate systems to the data warehouse environment. Patrick recognizes that the transition will require "working with users to determine their data needs, providing training on the new data warehouses, and coordinating with the campuses to ensure that the data in the warehouses is up-to-date and accurate."

Patrick Collins was the Executive Director of the California Census Research Data Center, a national data center located on both the Berkeley and Los Angeles campuses. Earlier, he was director of the National Data Archive on Child Abuse and Neglect at Cornell University. In both of these positions, he managed large-scale data depositories with a wide range of users, including University faculty and government researchers.

Patrick says, "In my previous position I managed a multi-campus operation and split my time between the Berkeley and UCLA campuses. I learned a lot about the mission and organization of the University. As a result, I bring to my new position an awareness of the uniqueness of the campuses. I have also seen how the decentralized nature of the University can make coordination across campuses difficult."

Patrick has also been involved in developing federal policy regarding management and sharing of scientific data and is involved in a state-funded project to draft model legislation concerning privacy and management of state administrative records in California.

Just Ask!

Ever since the "love bug" virus hit I've been afraid to open e-mail with attachments. Is there a safe way to do it?

Until last year, people felt safe opening e-mail attachments from people they corresponded with. That was before the debut of the Melissa virus — the first virus to send copies of itself to addresses in the victim's Microsoft Outlook address book. The recent love bug (AKA Love Letter or ILOVEYOU) virus and variants do the same thing. Eudora users will not spread this type of virus but they are just as vulnerable to its damaging effects.

The safest way to deal with suspicious e-mail attachments is to not open them until you've had the chance to scan them for viruses. To do this, note the name of the attached file and using the Eudora File Browser (in the Tools sub-menu of the Eudora Menu-bar) locate and right-click on it. In the resulting menu, select Command AntiVirus Scan. By default, attachments to Eudora e-mail notes are stored in the Eudora/Attach sub-directory.

Of course, this assumes that you have the very latest virus definition files available on your PC and that these include identifiers for the newest virus outbreak. IR&C maintains licenses for Command Software AntiVirus (formerly F-Prot) for all of OP and distributes updates frequently to PC Coordinators. If you are unsure whether you have the latest AntiVirus software, please contact your Departmental PC Coordinator.

In the case of the recent outbreaks, the required virus definition files would not have been available from Command Software until at least mid-day after the viral outbreak was discovered. In such a case, as soon as IR&C learns of a new virus outbreak, Workstation Support staff immediately strive to alert and advise all PC Coordinators as to the nature of the virus and the safest and most appropriate measures to take in dealing with it. In the case of the love bug virus, users were instructed not to open the attachment and to delete the note.

If you receive suspicious attachments after hearing on the morning (or previous evening's) news that a new virus outbreak has occurred, do not open the attachments, notify your PC Coordinator, and wait for his or her instructions.

David Wentworth

If you have questions for Just Ask! email Martha.Winnacker@ucop.edu

Records Management Committee Revises Disposition Schedules

The University Records Management Committee has embarked on a project to develop a new Records Disposition Schedules Manual for UC. The Schedules are guidelines for the University community on how long to retain administrative records, which records must be archived, and when records must be discarded. In addition to ensuring that necessary and valuable records are kept, the Schedules are important to the University because keeping records that are no longer needed increases the expense of storing and searching records.

The format of the current Manual was first developed in the 1960s and consists of detailed lists of individual forms and computer reports. The process that was originally developed for updating the Schedules is cumbersome and its complexity does not reflect the way the University does business today. Although the schedules for individual records have been updated periodically, many are out of date, compromising their usefulness to campus and UCOP offices. The purpose of revising the design of the Manual is to simplify the Schedules as well as to make it more flexible and easier to update in the future.

Alternative Approaches

The Committee looked at a number of methods of organizing records disposition schedules and selected a functional approach that aggregates records with similar characteristics into categories rather then enumerating them one by one. After looking at commercial products, the Committee chose instead to pattern the revised UC Manual after a model successfully used by another university.

The Oregon University System (OUS) serves the university, state college, and community college campuses in Oregon. In 1992 OUS undertook a systemwide overhaul of its records schedules, condensing eight separate manuals, some over 300 pages long, into one "functional" schedule with approximately 400 record groupings in 21 categories. By comparison, our Universitywide Manual lists approximately 1,300 individual records.

Conversion Plan

The first step taken by UC's Records Management Committee was to create a more concise list of fewer than 20 major groupings from the 61 categories into which the current UC Manual is divided. Between 200 and 300 sub-groups will then be identified.

The new top-level groupings are more descriptive of the function or process accomplished by the record, rather than being fragmented according to the particular office that utilizes the record. For example, where the current Manual has separate sections for Library Acquisitions, Storehouse, and Bookstore, as well as a section on "Purchasing & Disbursements," the revised Manual will have a section titled "Purchasing" that crosses all areas that have records pertaining to procurement of one type or another.

A sub-group of the Records Management Committee will pilot the functional method by identifying current individual listings that can be assigned to one or two of the new major groupings. The pilot will require input from operational managers at the campuses and functional experts at UCOP. In addition to getting their feedback on the appropriate retention period, their knowledge will be valuable in helping to identify records and processes that are not included in the current Manual. Any newly identified group of records that does not fit into the revised groupings will need to have retention schedules established once the mapping of Schedules into the new categories is completed. Assuming the pilot is successful, it is anticipated the entire project will be completed in approximately two years.

Criteria for Schedules

The Committee has established criteria for the new Records Disposition Schedules Manual. The Manual must stand alone, not as part of a Business and Finance Bulletin, so that it can be updated without a high-level review process. There also needs to be an easier mechanism for updating the Schedules in light of changing needs and records. Since campus policies may be more detailed or restrictive than Universitywide ones, the Universitywide Schedules must be designed to coordinate with local schedules. Finally, the Schedules should be online, so they will readily available to all staff who work with records, and must allow for glossary searches as well as drill-down menus.

The Committee is rewriting Business and Finance Bulletin RMP-2, which governs the records disposition program, in order to accommodate proposed changes in the Schedules and the procedures for updating them. The Committee plans to review other Business and Finance Bulletins in the Records Management Program (RMP) series over the next couple of years.

Connie Williams

CalREN2 Expands

CalREN-2, the advanced services Internet that replaced the UCNet intercampus network last year, is being extended through the Central Valley in preparation for the new UC Merced campus and in support of a number of UC facilities already in the Valley. The new "North-South link" will connect to CalREN-2 both in Los Angeles and in the Bay Area, providing a high speed north-south path independent of any external network.

The physical implementation of this new extension is being done in cooperation with the California State University system. Their existing 4CNet backbone is being upgraded to provide the additional capacity required by CalREN-2.

The fiber optic-based carrier services providing the 450 megabit per second circuits will pass through Bakersfield, Fresno, and Stockton. UC has facilities in each of these areas that will be connected to CalREN-2, including the UC Center in Fresno, the UCSF facilities in the Fresno Veterans Administration Hospital, the UC Merced Planning Office in Merced, and the UC Merced Learning Center in Bakersfield. In addition, the new UC Merced campus will be connected to the Stockton node before it opens in the Fall of 2004. The Central Valley North-South link should be operational by September.

A second phase of this expansion will connect Stockton to Sacramento to provide redundant connectivity to UC Davis. The new Sacramento node will also provide a termination point for the connection of the Nevada University and Community College System Network (UCCSN), expected to be completed by the end of the year.

Other pending connections include a redundant UCCSN connection in Anaheim and a connection to the Mexican Internet2 network being developed by the Corporación Universitaria para el Desarrollo de Internet (CUDI). The CUDI connection will be made at UC San Diego and is expected to be operational by August.

The CUDI connection is expected to enable closer collaboration with universities in Mexico, including the sharing of online information and teaching resources. A number of projects are already in place under the aegis of the UC Mexus project and Mexico's National Council on Science and Technology, El Consejo Nacional de Ciencia y Tecnologia (CONACYT). Such projects include studies of the health problems of cross-border Mexican workers and the economic impacts of the NAFTA agreement.

Future CalREN-2 projects include improved connection to Hawaii in support of the astronomer's using the Mauna Kea Observatory, and connection to Canada's Canarie network.

David Wasley

CDL Technology

continued from page 5

able to confirm that the requested material is not available on the user's campus by a real time check of the campus library circulation system (circulation checks are not yet available for UCLA or UCSB)

MyLibrary

MyLibrary is a prototype customization tool that will provide users with the ability to organize frequently used information resources in a personally meaningful way. Users will be able to create, store and manage customized "update" searches within specified resources or subject areas, create one-step pathways to frequently used reference tools, and activate CDL-hosted Databases Profiles. The test site for MyLibrary will be part of the CDL July release. MyLibrary will enable users to customize a CDL homepage for efficient access to resources they need regardless of the campus or collection in which the materials are held. Campus-specific views and branding will be possible via IP filtering. CDL's MyLibrary is based on the MyLibrary software developed at North Carolina State University. The CDL's version of MyLibrary will be built on the model developed by NCSU.

Support

CDL is accessible 24 hours a day, 7 days a week. Since campus libraries close at night and during parts of the weekend, technical support is provided at UCOP. IR&C staff in the Data Center monitor and maintain CDL systems around the clock. When trouble occurs, Data Center staff notify a CDL-T programmer who can usually intervene. Similarly, CDL users can send email to a UCOP helpdesk for assistance at any time.

Michael Thwaites

inside INFO

Published by: Information Resources and Communications, Martha Winnacker, Editor, University of California, 1111 Franklin Street, Oakland, CA 94607-5220. Email Martha.Winnacker@ucop.edu or telephone (510) 987-0409.