

MEMORANDUM

April 18, 2002

TO: Steve Bragg, Vice President for Finance and Planning
Al Goldfarb, Vice President and Provost
Susan Kern, Vice President for University Advancement
Helen Mamarchev, Vice President for Student Affairs

FROM: Dave Williams, Chair, Ad Hoc Committee on the USA Patriot Act

RE: Committee Report

[Report approved by the Vice Presidents, May 2002.]

In response to your request, a committee was convened in January to review the USA Patriot Act and its implications for campus operations. Members of the committee are:

Carolyn Bartlett, University Registrar
Bill Cummins, Director of Institutional Research
Wayne Ericson, Director of Student Health Services
Dan Hayden, Associate Vice President for Administrative Information System
Sarah Jome, Associate Director of International Studies
Ron Jones, Associate Vice President and Comptroller
Gary McGinnis, Associate Vice President for Graduate Studies, Research, & International Education
Rick Olshak, Director of Student Judicial Office
David Williams, Associate Vice President for Information Technology

The meetings of this group proved quite valuable not only in achieving the initial goal of studying the impact of USAPA but also in giving us a chance to share the day-to-day issues and responsibilities each of us confronts in managing privacy issues for the campus. Committee members contributed considerable time and effort to conduct a very thorough analysis of the issues. Attached please find a set of documents for your review:

- A. **USAPA Checklist for Illinois State University.** This document was based on a checklist prepared at UNC Chapel Hill. Our response to the checklist serves as the primary recommendations of the campus USAPA ad hoc committee. Checklist items #10 (legal review), and items #1, #7, and #8 are major recommendations for your review.
- B. **Implementation Quick Guides for Access to University Records and Communications.** This is the committee's response document for the two critical instances that may occur should a court-ordered request be submitted to anyone on campus. These guides should be distributed and promoted to all staff on campus.
- C. through G. Each of these documents is an assessment of the impact of USAPA on the following critical areas:
 - C. **FERPA**
 - D. **HIPAA**
 - E. **International Students**
 - F. **Electronic Data Security**
 - G. **Records Retention**

H. **Illinois State University Policies For Which a Review & Revision May Be Needed** . . . This includes a list of documents that merit review for consistency and USAPA issues.

I. **Data Custodians.** This is a first pass at documenting in one list the key administrators who have executive responsibility (as opposed to technical responsibility) for campus data, either paper or electronic form. This list should receive further review and editing by each Vice President.

Please let us know if you would like to discuss the report with the committee or if the committee can be of further assistance.

.

nh

Attachment

xc: Ad Hoc Committee on the USA Patriot Act

A. USAPA Checklist for Illinois State University

March 19, 2002

Prepared by the campus USAPA Study Group (David Williams, Chair; Carolyn Bartlett, , Bill Cummins, Wayne Ericson, Dan Hayden, Ron Jones, Sarah Jome, Gary McGinnis, and Rick Olshak).

Based on the David L. Harrison paper, "Surveillance and Monitoring of Technologies: New Privacy Issues After the USA Patriot Act," The University of North Carolina, Associate Vice President for Legal Affairs. January 2002.

1. Establish a protocol for all information requests. The USAPA committee has developed Guidelines (attached) for a campus-wide, unified response to any such information and communications requests and recommends that a training initiative be developed to train key staff and administrators in its implementation.
2. Establish or modify privacy policies. The campus USAPA committee has discussed the policies for electronic-data requests, FERPA related requests, HIPAA related requests, immigration related requests, and the retention of documents and financial information. A series of summaries of those policies and procedures (attached), and the impact that USAPA may have on those procedures has been prepared for the Vice Presidents to review. The committee also recommends that current University policies be reviewed as they relate to the issues addressed here (list attached).
3. Have a single point of entry for all information and surveillance requests. The committee has documented "major custodians" for information as well as the hierarchy of "custodians" under those administrators. All requests will be channeled through the appropriate "major custodian" of the data. The final point of entry, for any instance when the data custodian is unclear, is the University General Counsel.
4. Keep a confidential log of all information and surveillance activities. The committee recommends that all requests for information be report to the University's General Counsel and that that office maintain the log of information and surveillance activities.
5. Establish routines for surveillance activities and requests. The committee's response guidelines discussed in #1 above meets this requirement.
6. Establish emergency and computer trespasser procedures. The current system in place for the campus Appropriate Use Policy for computer activities provides a mechanism for dealing with these issues. The current custodians for the AUP policy are the Director of Student Technology Support Services and the AIS Data Security Administrator. These custodians maintain a tracking system of incident management concerning AUP.
7. Prevent disclosures or confidential breaches. The training component for #1 above should include a review of what staff are being asked to handle confidential information to ensure that staff are not being asked to deal with responsibilities beyond their job expectations. Further, that all staff are trained as to how to respond to any request by law enforcement for information of a sensitive nature.

8. Know what to look for when a request is made. The committee suggests we have a “town meeting” with local police, FBI, legal counsel, INS, etc. to discuss the USAPA issues and develop a collaborative environment with campus officials. Further, a larger staff training initiative may develop from this, where FBI and/or INS local staff could review and discuss models of typically types of requests for surveillance or information.
9. Conduct a capability study. A test of campus readiness would follow nicely after item #8 above. Periodic tests should be run to test readiness. Such tests could be designed in consultation with local and federal law enforcement officials.
10. Involve your legal counsel. Request that both the IBHE legal counsel and the campus counsel review the committee’s work and offer opinions; then, involve counsel in implementation plans and training.

B. Implementation Quick Guides for Access to University Records and Communications

March 19, 2002

I. How to respond to a court-ordered request for access to University records and communications.

Quick Guide: Only custodians are permitted to release or provide access to information.

First Responder

Anyone receiving a request for access to information should refer the requesting agent to the proper Custodian of Records. A list of Custodians is available at www.ilstu.edu/custodians, or in the A-Z index under “Custodians of Records.”

Custodian of Records

The Custodian of Records will copy proof of identification and the court order from the requesting agent and will contact General Counsel to establish a file for the request.

Upon direction from General Counsel, the Custodian will locate the materials requested, review them with the official requesting them and transmit copies as requested. Original documents may not be transmitted without approval by General Counsel.

All other requests for University information will be dealt with according to appropriate University Policies.

II. How to respond to Officials Requesting Court Ordered Interviews with University Constituents (Staff, Students)

Quick Guide: It is the policy of the University to encourage cooperation with such requests while providing reasonable protections of safety and comfort for University constituents.

First Responder

Anyone receiving a request for court ordered interviews will work with their supervisor to determine the proper level of response.

Supervisor

Supervisors will copy proof of identification and the court order from the requesting agent and will contact General Counsel to establish a file for the request.

Upon direction from General Counsel, the University will respond to the request, working with the interviewer and interviewee to establish reasonable protections of safety and comfort.

The University discourages interviews in private residences (including residence halls), individual offices, or off-campus public locations. University supervision may be provided by Campus officials, University Police, or legal counsel as determined by the interviewee and campus official.

**C. Response to Family Educational Rights and Privacy Act (FERPA)
Requests and Impact of U.S. Patriot Act (USAPA)**

April 2002

Impact: Very little impact on FERPA processes.

FERPA requests are handled consistent with the FERPA Guidelines and the Illinois State University Student Record Policy. A section on Confidentiality of Student Records is printed in the Graduate and Undergraduate Catalogs and the Class Registration Directory. The complete Student Record Policy can be found at www.policy.ilstu.edu/policydoees/records.htm. In addition, the memo to faculty sent with class list also includes a statement regarding confidentiality of student records.

All University Offices handling/storing Education Records are expected to follow the University guidelines.

The U.S. Patriot Act amends FERPA. Specifically it requires educational institutions to disclose education records to federal law enforcement officials without student consent in some circumstances. In such circumstances, the U.S. Attorney General or a U.S. Assistant Attorney General may obtain a court order that would require an educational institution to turn over education records considered relevant to a terrorism investigation if the official could certify that “specific and articulable facts” support the request. Additionally, the institution would not need to make a record of the disclosure, as FERPA normally requires.

Also included in USAPA is a provision that a college or university “shall not be liable to any person” for good faith disclosure of education records in response to such an order.

D. USA PATRIOT Act Impact on Release of Medical Information Procedures and Post-HIPAA Release of Medical Information Procedures

February 11, 2002

Degree of Impact: None

Summary of Current Release of Student Health Service Records

The Student Health Service medical record is the property of the Student Health Service and is kept for the benefit of the patient, the medical staff and the Health Service. However, the information contained within the record is the property of the patient and privileged information cannot be released to individuals, not otherwise authorized, without the written consent of the patient, a subpoena, a court order or statute. Original medical records shall not be taken outside of the Health Service. An exact duplicate is acceptable as evidence in a court of law. Any request for the original record should be referred to the Director of Patient Support Services.

The Student Health Service under appropriate circumstances without the patient's authorization can release nonprivileged information, i.e., information unrelated to treatment is considered nonprivileged. This data includes: name, address at time of treatment, age, sex, occupation or employer, dates of admission, discharge or outpatient visits, verification of visits to the Student Health Service, general condition on discharge (alive or expired), name and address of next of kin, name of attending physician (not the specialty of the physician). The specialty of service classification of the attending physician is privileged information and should not be disclosed.

Discretion should be used so that information is not revealed to persons without a legitimate reason. Any information other than the above is considered privileged and is not to be released without valid written authorization (see HS-0515).

Summary of Release of Student Health Service Records after HIPAA

Each patient will sign a *Consent to the Use and Disclosure of Health Information for Treatment, Payment, or Healthcare Operations* form and receive a *Notice of Information Practices* prior to or at their first clinic visit following the implementation of HIPAA Privacy Rules (April, 2003). ISU SHS may release patient records for the purpose of treatment, payment and health care operations without obtaining a separate authorization from the patient.

ISU SHS must have a signed Business Associate agreement with other entities with which it shares individually identifiable health information. This agreement requires that a Business Associate of SHS meet all the requirements of HIPAA. Examples of SHS Business Associates may include Quest reference laboratory, Bloomington Radiology, PyraMED by Media Highway (clinic management system), QS1 Pharmacy Software, etc.

SHS may disclose health information for law enforcement purposes as required by law or in response to a valid subpoena or court order. If there is any question regarding the release of medical information, SHS will verify subpoena, court order or other law enforcement requests with the Office of General Counsel.

To the best of our knowledge HIPAA and release of medical records/information are not mentioned in the USA PATRIOT Act. However, there may be an incidental link between these acts if health information is stored on a computer to be inspected by authorities under the USA PATRIOT Act.

Note: SHS Medical records are excluded from FERPA

Prepared by Laura Knoblauch and Wayne H. Ericson

E. International Students and FERPA

April 2002

Impact: The only anticipated impact the Patriot Act will have on international students at ISU is that there may be an increase in the frequency of contact from the FBI. In the past, the FBI has only contacted the International Office about once a year. We will also make an extra effort to make sure that all official international visitors to ISU check in with our office as this does not always happen.

Requirements

Immigration and Naturalization Service (INS) regulations, part of the U.S. Department of Justice, require that certain information must be kept on F-1 students, that schools must release this information to INS officers and that schools must periodically report this information to INS.

The required information includes

- Name
- Date and place of birth
- Country of citizenship
- Address
- Status (full-time or part-time)
- Date of commencement of studies
- Degree program and field of study
- Whether the student has been certified for practical training and the beginning and ending dates of certification
- Date of termination of studies and reason, if known
- The documents the school needed to review to issue an I-20 AB
- Number of credits completed each semester
- Photocopy of the student's I-20 ID

This information can be held in numerous places (i.e. the Admissions Office and the Registrar's Office) but must be accessible to the international office. The international office keeps copies of student's passports, I-94 cards, I-20s, IAP-66s, as well as applications for various immigration benefits like employment. These documents contain all the information that we know will not be found in the Registrar's or Admissions Offices.

(Note: There are 7-10 other non-immigrant classifications of students enrolled at Illinois State in any given semester. The Office of International Studies and Programs (OISP) track the same information for them as they do for the F-1 students. The OISP does not regularly track information on students in various immigrant classifications.)

(Note: Other information that is requested for the annual census but which is not required by INS includes gender, main source of funding and marital status.)

Retention

The university must maintain the required information mentioned above on each F-1 student during the entire time the student attends the institution and until the school completes any required reports to the INS. (Note: The INS has not requested that schools report this information since 1988. The mechanism to report this was a very cumbersome paper/pencil process which is planned to be replaced by the CIPRISS/SEVIS program.)

Release of information

INS may request any or all of the information required to be kept on any individual student or class of students, upon notice to the school. The school must respond to such requests, and may not insist on a subpoena. A school has 3 working days to respond to any request for information concerning an individual student and 10 working days to respond to any request for information concerning a class of students (e.g. all students from a particular country).

INS's request for information must be in writing if the school asks for a written request, but if INS seeks information on a student who is being held in custody, the school must reply orally on the same day although the school may request INS to provide written notification that the request had been made. Failure to comply with the request for information constitutes cause for withdrawal on notice of the school's approval to enroll nonimmigrant students.

(Note: It is important to *understand that regulations require the release of only the information specified and only to an INS officer in the manner described. They do not require or authorize the release of any information to anyone else, including representatives of other government agencies who may occasionally ask for information about students from abroad.*)

Legal Considerations

FERPA allows release of directory information which is usually defined as name, address, telephone number, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended.

IIRAIRA altered the application of FERPA to international students and scholars, but only as these matters touch on CIPRISS/SEVIS. At this time, there are no regulations to explain how these two laws will interact. Advisers should approach FERPA issues in the same manner as they have in the past – i.e. assume that international students and scholars are protected by FERPA for all inquiries outside the narrowly defined INS inquiry structure already defined.

Whether a school should provide information about students for whom the school is not required to maintain records for immigration purposes is a decision to be made in consultation with legal counsel.

Most of this information is taken directly from the NAFSA Adviser's Manual.

F. Electronic Data Security Issues and the USA Patriot Act

April 2002

This document summarizes overall campus security issues related to computer workstations, servers, databases, telephone switches, and voice mail storage systems and evaluates the impact of the USA Patriot Act on in-place procedures.

Impact: The USA Patriot act raises the following issues related to in-place procedures for computing and data storage on the Illinois State campus. All of these may not be directly relevant to the USAPA, but the USAPA reinforces the need for examining security for campus data as well as a request for information or surveillance:

- Need for greater standardization of response procedures to a likely increase in requests from law enforcement for access to log files, email or news postings, and, on individual workstations, contents of caches, history logs, emails, voice mail, phone logs, and computer files (including those that have been deleted but are recoverable).
- Need for specifying expiration dates for computer server log files based on the shortest time relative to when those logs are “no longer needed” for operations (the State of Illinois does not appear to have retention guidelines for server logs) and to set retention times for server and telephone switch backup files for critical operations.
- Need to review and revise campus policies related to the security of electronically storing confidential student, medical, and personnel information to ensure that the procedures use state-of-the-art technology and reflect the current organization of campus computing.
- Need to communicate campus policy and procedures regarding the storage and security of confidential information cover by FERPA and HIPAA on workstations and servers, especially for those computers that are maintained by various campus units, apart from AIS and CTSG supervision.
- Need for staff preparedness on law enforcement requests or implementing without notice email wiretaps (e.g., FBI’s Carnivore software) and keystroke monitoring on computer workstations.

Below is a summary of how security is handled for key computer operations on campus. The current response for any request of information from law-enforcement is to cooperate fully and to notify appropriate campus officials.

PC Workstation Security Procedures. Individual PC workstations on campus present the least secure of all computing environments and one of the more likely targets for law-enforcement electronic searches. The person responsible for the data and/or information stored on these PCs is the person who operates or uses that PC. These users should be aware of the campus Acceptable Use Policy and should also be aware that any data stored on their PC is the property of Illinois State University and that the privacy and security of that data is not guaranteed. Users should be aware of policies and procedures related to the protection of the privacy of student information (FERPA), medical information (HIPAA, and other personal information and should not store this kind of information on insecure servers. An individual’s PC contains files (including those that have been deleted, but can be reconstructed), software caches, logs, email, Web browsing histories and bookmarks, that can collectively be used to determine fairly accurately what a person has been doing on a workstation. The use of Entrust PKI encryption, frequent erasing of cache and history files, and the use of software “shredding” techniques can greatly reduce traceable materials on a PC (an example is the “TrueDelete” feature to the Entrust desktop suite. If confidential data has been encrypted with the State’s Entrust PKI technology, law enforcement officials will have to request access to the private keys from the State of Illinois to view these files.

For the many public workstations accessible through campus labs and walk-up stations, these machines are frequently “ghosted” (essentially rebuilding the hard drive and erasing all files) and are not likely to leave any evidence of a user’s work pattern after a week or less.

Unit Server Procedures. Most departments and service units on campus have a server or two running everything from mailing list databases, to inventory, to web-based forms for acquiring and accessing data. These units are maintained locally and are not under the supervision of central AIS and CTSG server management. It is not known to what extent these servers are storing confidential data and what security procedures are in place to protect that data. A concerted effort needs to take place, through a combination of policy revision and education, to ensure that local units maintain the same level of security as AIS and CTSG. Campus-wide decisions on the retention of log files should include local area servers as well.

Mainframe Security (AIS). The campus mainframe data is protected through industry standard RACAF security procedures based on explicit authorization for each transaction used to access to the data. This authorization to run a transaction is approved by the data custodian for that transaction and enforced by the RACAF facility on the mainframe. There are currently only 46 designated data custodians (see attached list) who can approve a request for access to mainframe transactions (and ultimately to the data these transactions retrieve). These custodians are the people who should ultimately approve or disapprove all access requests including those from external entities and law enforcement agencies or courts.

Student programming on the mainframe is completely isolated in a separate virtual space apart from the systems production area. Log file retention needs to be evaluated in the mainframe area as for other servers on campus however, since some of the mainframe log files are used for chargeback purposes, their retention period may be up to one year. It is important to retain an audit trail for the chargeback system.

Campus Internet Server Security (CTSG). The majority of campus-wide servers supporting email, web, newsgroups, curriculum management software, the iCampus portal, computer directory (LDAP) fall under CTSG and are managed by the Computer Infrastructure Support Services (CISS). There are a number of security issues in place to protect access to these data, and to protect the misuse of these resources for launching illegal or harassing Internet activity (either from campus, or masquerading as a user on campus).

The campus Internet servers and their access to confidential information (passwords, social security numbers, student and personnel information (beyond what appears in the campus phonebook) are protected through a network of virtual local area networks (VLANS) that isolate key server activity from public activity. Primary, confidential information is stored on LDAP directories and these are highly secure.

The master LDAP directory is isolated via VLAN and contains all information needed for running Internet server applications. No applications interact directly with this master LDAP. Sub-LDAP directories are used on a “need to know basis” with specific applications; these sub-directories contain only the LDAP information necessary for that specific application. Other servers on campus may have access to key LDAP directory resources after rigorous controls have been established to ensure data security.

Access to campus email, web, and other Internet servers is also protected by VLAN architecture making it extremely difficult for illegal access to these data.

Two other security risks are the illegal use of campus ULIDs and the use of campus mail servers in masquerading falsely as someone on campus. Stringent monitoring of “open relays” on campus mail servers ensures that someone cannot send email from one of our mail servers without having a valid

ULID on campus. We do not currently implement “authenticated” mail. This means that someone on campus could falsely send mail using someone else’s ULID.

ISUnet and Campus Telephone Security (CTSG). The University telephone system and the campus network (ISUNet) as is managed by Telecommunications and Network Support Services (TNSS). The campus has various devices and systems that monitor traffic, but no systems are used, or intend to be used, to monitor content. Wiretaps for phones and their equivalent for networks would be required to monitor content.

At the present time legal wiretaps require a court order and are processed through University legal counsel per University policy and the technical aspects of the wiretap placement would be coordinated with TNSS. Federal authorities may at some point also require the University to allow the permanent attachment of special hardware to University telephone and data networks to permit internal wiretaps to be remotely activated by federal authorities without University intervention or knowledge. Illegal wiretapping within the University would require attachment to the University telephone system wiring or the placement of wireless transmission devices on or near telephone instruments. Most administrative telephones use digital technology for their voice transmissions and a higher than normal expertise would be required to actually monitor these conversations. Remote access to the actual telephone switching equipment is protected through software and passwords restrictions and the physical equipment is located in locked areas.

ISUnet Security

Data exchanged between any network host and client residing on ISUnet is protected from capture through the use of switched Ethernet and VLANs. In a typical switched Ethernet environment, only the sender and receiver have access to data transmitted between them. Data exchanged between a campus-based host and a client using a third party ISP can potentially be captured. Through the implementation of our coming VPN (Virtual Private Network) solution, a client can access a campus host through an authenticated session running over an encrypted software tunnel. These data cannot be decrypted by any device other than the sender and receiver. Data exchanged between a client associated with a wireless access point and a host can be vulnerable without appropriate security measures. To address this issue, a standards-based authentication and encryption model has been implemented on ISUnet. Only wireless cards that support these techniques can associate to a campus wireless access point.

There are a variety of measures on ISUnet used to protect campus-based hosts from exploitation. These include anti-address spoofing countermeasures throughout the network, and access control lists to block applications that are well-known security risks between ISUnet and our service providers. IP source routing (the source defines the route between sender and receiver) and directed broadcasts (sending messages to a broadcast address) are not supported on ISUnet to prevent the sender from diverting traffic to an unexpected receiver. To provide an almost unlimited amount of IP address space for ISUnet users, private IP addressing has been implemented on ResNet, University affiliated residential broadband networks (i.e.: ADSL from Verizon), wireless networks, public access networks, or any campus Ethernet network where DHCP is used. Because private IP addresses are not known to clients or hosts using a third party ISP, it is difficult to gain access to a campus-based resource residing in private IP address space.

Users of the campus dialup, public network jacks, ResNet, or wireless network must have a valid ULID to connect. All authentication systems are logged to provide the means for tracking user access over time; the logs are only kept for a finite amount of time before being discarded.

G. Records Retention Summary for Illinois State University

Degree of Impact: The State of Illinois Archives Office has no retention schedules established for server logs and other similar electronic files. It is therefore the responsibility of Illinois State University to establish its own retention schedule. Any electronic files that replace paper files are to be retained for the same period of time that the original paper documents would have been retained.

On December 8, 1992 the Records Management Section of the State of Illinois Archives Office completed a very exhaustive review of all University records. This review lasted several months and resulted in a large manual consisting of retention requirements for documents created and maintained by all University offices and departments.

The review addressed practically every piece of paper on this campus but did not address electronic files. Even the review of Administrative Computing addressed only the "business" portion of the office such as the retention of software maintenance contracts etc.

It is impossible to summarize this extensive analysis into one page but it was very rare to have any retention requirement extend beyond 5 years. If there was a requirement to retain beyond five years it was usually for such items that should be retained indefinitely such as student course grades. Therefore five years could be established as a safe default for new documents and reports not specifically itemized on the original study.

Some source records, such as daily paper check registers in the Comptrollers Office, have been converted from paper to electronic files. When a specific paper document with a stated retention length no longer exists, its electronic counterpart should be maintained for the same retention requirement.

**H. Illinois State University Policies For Which A Review & Revision
May Be Needed Prior to Next Review Cycle Due to
Passage of USA Patriot Act**

April 2002

Reference	Policy Title	Contact Office	Next Review Cycle
1.1.7	Use of Electronic Equipment For Surveillance Purposes	Vice President & Provost	2005-06
8.4.13	Special Internal Call Tracking	Office of Telecommunications	No date given
2.1.1	Student Records	Office of University Registrar	2002-03
8.2.1	Appropriate Use Policy	Data Security Administrator	2003-04
8.2.2	Information Resource Access & Security	Data Security Administrator	2001-02
8.2.5	Code of Responsibility For And Confidentiality of Data	Data Security Administrator	2001-02
8.2.9	Lan Coordinator's Standards & Guidelines For Secure Environment	Data Security Administrator	2001-02

**I. Illinois State University
Executive/Major Custodian of University Data/Records**

<u>Office</u>	<u>Location</u>	<u>Custodian/ Privacy Administrator</u>	<u>Current</u>	<u>Type</u>
President	418 Hovey	President	Victor Boschini	Lead Administrator
Redbird Arena	Redbird Arena	Assistant Director*	Cynthia Harris	Athletic
Redbird Arena	Redbird Arena	Events Administrator*	Rebecca Short	Athletic
Athletics	213 Redbird Arena	Director	Perk Weisenburger	Misc.
<u>Vice President Finance & Planning</u>	302 Hovey	Vice President*	Steve Bragg	Lead Administrator
Parking Services	Parking Services Bldg	Director*	Bob Nuckolls	Auto Registration
Vice President for Finance & Planning	302 Hovey	Budget Officer*	Barbara Blake	Financial
Comptroller	302 Hovey	Comptroller	Ron Jones	Financial
Comptroller	102 Hovey	Assistant Comptroller	JoEllen Bahnsen	Financial
Student Accounts	607 W. Dry Grove	Collection Specialist*	Doug White	Financial
Student Accounts	607 W. Dry Grove	Bursar *	Greg Lyle	Financial
Redbird Card Office	215D Bone Student Center	Coordinator	Robin Knapp	Identification
Insurance (Student)	230 Student Services Bldg.	Supervisor	Bonnie Crutchley	Insurance
Facilities Management		Manager *	Shane Brown	Inventory
Mail Service	104 Nelson Smith Building	Manager*	Elizabeth Spelios	Mail
Central Receiving		Inventory Specialist*	Al Meister	Materials
Human Resources	101G Nelson Smith Building	Human Resource Officer*	Tom Fowles	Personnel-Civil Service
Administrative Information Systems	101 Julian Hall	Assistant Vice President*	Danney Hayden	System
Administrative Information Systems	120 Julian Hall	Manager*	Heather Dehn	System
Administrative Information Systems	102 Julian Hall	Manager*	Jay Anderson	System

**I. Illinois State University
Executive/Major Custodian of University Data/Records**

<u>Office</u>	<u>Location</u>	<u>Custodian/ Privacy Administrator</u>	<u>Current</u>	<u>Type</u>
<u>Vice President for University Advancement</u>	401 Hovey	Vice President	Susan Kern	Lead Administrator
Advancement Services	222 Rambo House	Specialist*	Ellyce Wolfe	Financial
<u>University Advancement</u>	401 Hovey	Vice President*	Susan Kern	Financial
Printing Services	101 Nelson Smith Building	Director*	David Nelson	Print Media
<u>Vice President for Student Affairs</u>	301 Hovey	Vice President	Helen Mamarchev	Lead Administrator
Student Life	387 Student Services Bldg.	Director	Jill Benson	Activities
Student Dispute Resolution Services	202 Fell Hall	Director	Richard Olshak	Disciplinary
Disability Concerns	350 Fell Hall	Director	Ann Caldwell	Health
Student Health Service	214 Student Services	Medical Records Adm.	Laura Knoblauch	Health
Student Health Service	303 Student Services Bldg.	Director *	Wayne Ericson	Health
Student & Alumni Placement Services	110 Student Services Bldg	Adm. Assistant *	Joseph Miller	Placement
Student & Alumni Placement Services	185 Student Services Bldg.	Director	Pamela Hammond-McDavid	Placement
University Housing Services	ORL Building	Administrative Clerk*	Connie Guhlstorf	Residential
University Housing Services	ORL Building	Director	Maureen Blair	Residential
University Housing Services	ORL Building	Administrative Clerk*	Robyn McGownd	Residential
<u>Vice President & Provost</u>	410 Hovey	Vice President Provost	Alvin Goldfarb	Lead Administrator
Academic Advisement	340 Fell Hall	Director *	Mike McElyea	Academic
Undergraduate Studies	308 Hovey	Asst. to Associate Vice President*	Sally Pyne	Academic
Honors Program	North & Fell Streets	Director	Steve Rosenbaum	Academic
Financial Aid	231 Fell Hall	Director	Charles Boudreau	Financial
Financial Aid	244 Fell Hall	Associate Director*	Jon Gudenrath	Financial

**I. Illinois State University
Executive/Major Custodian of University Data/Records**

<u>Office</u>	<u>Location</u>	<u>Custodian/ Privacy Administrator</u>	<u>Current</u>	<u>Type</u>
Milner Library	Milner Library	Associate Professor *	Richard Christensen	Library Materials
Orientation	328 Fell	Coordinator	Mary Jo Fabich	Participation
Academic Personnel	207 Hovey	Procedures & Systems Manager *	Rama Suresh	Personnel -Academic
Extended University	4090 Extended University	Director	Galen Crow	Program Participation
Graduate School	310 Hovey Hall	Associate Vice President	Gary McGinnis	Academic
Research Office	310 Hovey Hall	Associate Vice President	Gary McGinnis	Academic
Graduate School	310 Hovey	Admission & Records Officer *	Mary Stack	Academic
Graduate School	310 Hovey Hall	Director	Sandy Little	Academic
International Studies	308 Fell Hall	Coordinator *	Kelly Mirsky	Academic
International Studies	308 Fell Hall	Director	Momar Ndiaye	Academic
International Studies	308 Fell Hall	Coordinator	Sarah Jome	Immigration
Office of University Registrar	First Floor Moulton Hall	Registrar *	Carolyn Bartlett	Academic
Office of University Registrar	First Floor Moulton Hall	Associate Registrar	Edward Mayer	Academic
Admissions	201 Hovey Hall	Director	Steve Adams	Admission
Scheduling	109 Moulton Hall	Adm. Assistant*	Roberta Thomas	Course/Room Scheduling
Campus Technology Services	411 Hovey	Acting Associate Vice President*	David Williams	Systems
Computer Infrastructure Support Services	154 Julian Hall	Director	Carla Birkelbaw	Internet
Computer Infrastructure Support Services	154 Julian Hall	Associate Director	Rudy Radosovich	Internet - E-mail, Web
Telecommunications	105 Williams Hall Annex	Director	William Blomgren	Telecommunications
<u>College of Applied Science & Technology</u>	145 Turner	Dean	Robert Rossman	Academic

**I. Illinois State University
Executive/Major Custodian of University Data/Records**

<u>Office</u>	<u>Location</u>	<u>Custodian/ Privacy Administrator</u>	<u>Current</u>	<u>Type</u>
Kinesiology & Recreation School of	214 Horton	Chairperson	Alan Lacy	Academic
Military Science	102 House on Univ. Ave.	Chairperson	Dominic Lilak	Academic
Health Sciences	305 Felmley	Chairperson	Marilyn Morrow	Academic
Agriculture	150 Turner	Chairperson	Randy Winter	Academic
Applied Computer Science	133 Stevenson	Chairperson *	Robert Zant	Academic
Family & Consumer Sciences	144 Turner	Chairperson	Susan Winchip	Academic
Criminal Justice Science	401 Schroeder	Chairperson	Thomas Ellsworth	Academic
Technology	210 Turner	Chairperson	Rod Custer	Academic
Applied Computer Science	133 Stevenson	Lecturer *	Sally Scott	Academic
<u>College of Arts & Sciences</u>	141 Stevenson	Dean	John Freed	Academic
Speech Pathology & Audiology	204 Fairchild	Chairperson	Al Bowman	Academic
Foreign Languages	412 Stevenson	Chairperson	Barbara Kurtz	Academic
Mathematics	313 Stevenson	Chairperson	Catherine Kinsky	Academic
Psychology	435 DeGarmo	Chairperson	David Barone	Academic
Geography/Geology	206 Schroeder	Chairperson	David Malone	Academic
Economics	425 Stevenson	Chairperson	David Ramsey	Academic
Physics	311 Moulton	Chairperson	George Rutherford	Academic
Politics & Government	306 Schroeder	Chairperson	Jamal Nassar	Academic
Philosophy	351 Stevenson	Chairperson	James Swindler	Academic
Communication	434 Fell Hall	Chairperson	Larry Long	Academic
Chemistry	305 Felmley	Chairperson	Michael Kurz	Academic

**I. Illinois State University
Executive/Major Custodian of University Data/Records**

<u>Office</u>	<u>Location</u>	<u>Custodian/ Privacy Administrator</u>	<u>Current</u>	<u>Type</u>
Sociology- Anthropology	338 Schroeder	Chairperson	Nick Maroules	Academic
History	334 Schroeder	Chairperson	Paul Holsinger	Academic
School of Social Work	363 Schroeder	Director	Richard Grinell	Academic
English	409 Stevenson	Chairperson	Ron Fortune	Academic
Biological Sciences	206 Felmley	Chairperson	Tak Cheung	Academic
<u>College of Business</u>	315E Williams	Dean	Dixie Mills	Academic
Finance, Insurance & Law	328 Williams	Chairperson	Charles McGuire	Academic
Accounting	435A Stevenson	Chairperson	James Moon	Academic
Management & Quantitative Methods	329 Williams	Chairperson	John Lust	Academic
Marketing	325 Williams	Chairperson	Tim Longfellow	Academic
<u>College of Education</u>	506 DeGarmo	Dean	Dianne Ashby	Academic
Clinical Experience Certification Processes	DeGarmo Hall	Director *	Deborah Curtis	Academic
Clinical Experience Certification Processes	DeGarmo Hall	Coordinator*	Lucille Buscher	Academic
Educ. Admin. & Foundations	311 DeGarmo	Chairperson	Patricia Klass	Academic
Curriculum & Instruction	232 DeGarmo	Chairperson	Rex Morrow	Academic
Specialized Educational Development	533 DeGarmo	Chairperson	Jim Thompson	Academic
<u>College of Fine Arts</u>	116 Center/Visual Arts	Dean	Roosevelt Newson Jr.	Academic
School of Theatre	212 Centennial West	Director	Fergus Currie	Academic
School of Music	230 Centennial East	Director	James Major	Academic
School of Art	119 Center/Visual Arts	Director	Ron Mottram	Academic

**I. Illinois State University
Executive/Major Custodian of University Data/Records**

<u>Office</u>	<u>Location</u>	<u>Custodian/ Privacy Administrator</u>	<u>Current</u>	<u>Type</u>
Mennonite College of Nursing	312 Edwards	Dean *	Nancy Ridenour	Academic
Nursing Programs	312 Edwards	Director	Nancy Ridenour	Academic