NACUBO
Advisory Report 2003-02

March 13, 2003

COMPLIANCE WITH NEW DOMESTIC SECURITY LEGISLATION

This report is a joint undertaking of the American Council on Education (ACE) and the National Association of College and University Business Officers (NACUBO). It represents an effort to provide college presidents, provosts, business officers, and other senior administrators with an overview of provisions in several new laws passed in the aftermath of the September 2001 terrorist attacks that impact colleges and universities. ACE and NACUBO have endeavored to keep members informed of changing requirements as they developed. This report provides a summary organized by administrative departments on campus.

The report was prepared by the law firm of Hogan & Hartson LLP. The primary authors were Martin Michaelson and Deborah T. Ashford, with assistance from Paul W. Virtue, Catherine R. Guttman-McCabe, Stephanie J. Gold, and Michael J. Vernick.

Introduction

College and university presidents, provosts, business officers, and other senior administrators need to be aware that a number of post 9-11 legal enactments and government agency actions impose significant new burdens on their staffs. Specifically, three major anti-terrorism-related statutes enacted by Congress since September 11, 2001, pertain to higher education:

1. The **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act, or USAP)**, P.L. 107-56 (Oct. 26, 2001), enhances the power of law enforcement to combat terrorism through surveillance and other information-gathering techniques and lays the groundwork for subsequent immigration and bioterrorism legislation.

2. The **Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act, or BSA)**, P.L. 107-173 (May 14, 2002), addresses monitoring of and data collection regarding foreign students, including establishment of an Internet-based information system. Subsequent Immigration and Naturalization Service (INS) and Department of State administrative actions on May 16, September 18, and September 25, 2002, further these objectives.

3. **The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (BPRA)**, P.L. 107-188 (June 12, 2002), spurs development of new therapeutic products to combat bioterrorism, strengthens federal oversight of biological agents and toxins, and establishes new management goals for the Food and Drug Administration that will have a major impact on drug and biological product approval.

These new areas of anti-terrorism-related regulation have developed rapidly, and many issues remain in flux. Institutional offices are advised to consult their legal counsel regarding these and forthcoming legal developments.

The purpose of this report is twofold: (1) to summarize these new laws and administrative agency actions as they pertain to higher education, and (2) to provide an in-depth review of key actions and responsibilities required by institutional offices or functions that are likely to be primarily affected by these new laws—namely, the registrar, the foreign student office, information technology officials, officials who process subpoenas and war-

rants, research administrators, and environmental health and safety officers.

In brief, the following institutional offices or functions should be knowledgeable about and take actions in the areas indicated below. Subsequent sections of the report, beginning on the page indicated, provide greater detail.

Responsibilities in Brief

- **Registrar and Others Who Maintain Student Records** (page 3)
  - New authority for court-ordered disclosure of education records
  - Federal law enforcement collection of student information from the National Center for Education Statistics
- **Foreign Student Advisors** (page 5)
  - Increased monitoring of foreign students
  - Student and Exchange Visitor Information System (SEVIS) implement-ation and deadlines
  - Interim Student and Exchange Authentication System (ISEAS) requirements and deadlines
  - Immigration and Naturalization Service (INS)* compliance reviews
  - Proposed regulatory changes regarding student status
  - Commuter status for part-time students
- **Information Technology Officials and Officials Who Process Subpoenas and Warrants** (page 11)
  - Authority to seize stored voice-mail messages
  - Required disclosure of electronic communications or records
  - Court orders for Internet surveillance
  - Compelled disclosure of "any tangible things"
  - Voluntary disclosure of electronic communications or records
  - "Computer trespasser" provision
  - Computer-hacking penalties
  - Nationwide search warrants
  - Court orders for education records
- **Research Administrators and Environmental Health and Safety Officers** (page 14)
  - Penalties for improper possession of or delivery systems for dangerous substances
  - New regulations regarding access to, use, and transfer of certain biological "select agents"

* The Immigration and Naturalization Service (INS) was abolished effective March 1, 2003, and its functions were folded into three separate bureaus within the Department of Homeland Security (DHS). The Bureau for Citizenship and Immigration Services (BCIS) will share responsibility for student and schools issues with the Bureau for Imiigration and Customs Enforcement (BICE). BICE will have responsibility for administration of the Student and Exchange Visitor Information System (SEVIS) while BCIS will be responsible for student visas issues. Historical references to INS are maintained. For references to agency authority continuing after March 1, 2003, we use the terms Department of Homeland Security or DHS.

Registrar and Others Who Maintain Student Records

The USA Patriot Act (USAP) amends the Family Educational Rights and Privacy Act (FERPA) to permit educational institutions to disclose education records to federal law enforcement officials without student consent as follows:

- ➲ By certifying that "specific and articulable facts" support the request, a U.S. Assistant Attorney General or higher-ranking official may obtain an ex parte court order that requires an educational institution to turn over education records considered relevant to a terrorism investigation.
  - Institutions do not violate FERPA by responding to such an order without student consent.
  - The institution need not make a record of the disclosure, as FERPA ordinarily requires.
  - A college or university "shall not be liable to any person" for good faith disclosure of education records in response to such an *ex parte* order.

USAP does not explicitly amend FERPA's "health or safety emergency" exception. Recent U.S. Department of Education guidance suggests that the health or safety emergency exception is limited, but may be applied in the case of a bioterrorism attack or another attack like that on September 11, 2001.

USAP also permits federal law enforcement officials to collect from the National Center for Education Statistics individually identifiable student information that would otherwise be subject to strict confidentiality standards.

Individuals who maintain student education records must understand how the USAP amends FERPA. In addition, individuals who maintain student education records must understand preexisting FERPA requirements that may be relevant to law enforcement requests for such records. The chart on page 4 summarizes select FERPA provisions related to law enforcement requests, including the recent USAP amendment, and addresses whether prior notice, consent, and record keeping are required.

Requests for Student Records After the USA Patriot Act:

Notice, Consent, and Record-Keeping Requirements Under Select FERPA Provisions

Select FERPA Provisions	Prior Notice and Consent Required?	Record Keeping Required?
Records that an institution's law enforcement unit creates and maintains for a law enforcement purpose may be disclosed.	No.	No.
Unless a student has opted not to have his or her directory information disclosed, an institution may disclose "directory information" (e.g., a student's name, address, telephone listing, e-mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status, participation in officially recognized activities or sports, weight and height of members of athletic teams, degree, honors and awards received, and most recent institution attended).	No.	No.
In an emergency, personal information in education records may be disclosed if knowledge of such information is necessary to protect the health or safety of the student or other individuals.	No.	Yes.
Education records may be disclosed to comply with a judicial order or pursant to a lawfully issued subpoena.	Yes, prior notice. No, prior consent.	Yes.
Education records may be disclosed without student consent or prior notice in response to: ➲ a federal grand jury subpoena, if the court orders, for good cause shown, that the institution not disclose the existence or contents of the subpoena or any information furnished to the grand jury in response to the subpoena; and ➲ any other subpoena issued for a law enforcement purpose, if the court or other issuing agency orders, for good cause shown, that the institution not disclose the existence or contents of the subpoena or any information furnished in response to the subpoena.	No.	No.
Education records may be disclosed to the U.S. Attorney General or his or her designee in response to an *ex parte* order issued under the Patriot Act's FERPA amendment.	No.	No.

Foreign Student Advisors

The USA Patriot Act (USAP) calls for full implementation and expansion to all foreign students (other than those who hold immigrant visas) of existing law—not enforced to date by the federal government to the extent of its authority—that permits federal agencies to collect from colleges and universities information about such students. The information includes name and address, visa classification and issuance or extension date, full-time enrollment status, and disciplinary action resulting from criminal conviction. Such disclosures are exempt from FERPA under existing law.

Several recent regulatory and legislative developments have substantially impacted foreign student programs at educational institutions with F-1, M-1, or J-1 nonimmigrant students.

1. On May 14, 2002, President Bush signed into law the **Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act, or BSA)**. Sections 501 and 502 of this legislation address enhanced monitoring of foreign students and amend section 641 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA).

2. On May 16, 2002, the INS published a proposed regulation to change the means by which information about foreign students and exchange visitors is retained and reported and to implement the **Student and Exchange Visitor Information System (SEVIS)** 67 Fed. Reg. 34862. The proposed regulation reflects statutory mandates set forth in section 641 of IIRIRA (8 U.S.C. § 1372); the USAP, P.L. 107-56, enacted October 26, 2001; and the BSA.

3. On September 18, 2002, the Department of State (DOS) issued an interim rule creating an electronic system known as the **Interim Student and Exchange Authentication System (ISEAS)** to implement the transitional requirements of the BSA related to monitoring of foreign students and exchange visitors prior to full implementation of SEVIS. 67 Fed. Reg. 58693.

4. On September 25, 2002, the INS issued an interim rule related to review and certification of INS-approved educational institutions in connection with SEVIS. 67 Fed. Reg. 60107.

5. On December 11, 2002, the INS issued final regulations on SEVIS implementation, establishing a January 30, 2003, deadline for institutions to switch over to the new system for all new or modified I-20s. 67 Fed. Reg. 76256. On January 1, 2003, the INS granted a grace period for compliance until February 15, 2003.

Relevant provisions of the BSA as well as the interim and final rules are summarized below.

Enhanced Border Security and Visa Entry Reform Act of 2002

In amending Section 641 of IIRIRA, the BSA order Security Act requires the Attorney General and the Secretary of State to establish an electronic system to monitor and verify:

- issuance of documentation by an educational institution that accepts a foreign student into its programs;
- issuance of a visa to a foreign student;
- admission of a foreign student into the country;
- notification to the educational institution that the foreign student has been admitted into the country;
- registration and enrollment of the foreign student in the educational institution; and
- other relevant actions of the foreign student, such as change of school or termination of studies.

To jumpstart foreign student monitoring reforms while implementation of these pro-visions continues, the BSA mandated establishment of a transitional program now known as ISEAS (described in detail below).

Section 641 of IIRIRA previously required approved educational institutions to collect the following information about foreign students in F, J, or M status:

- identity and current U.S. address;

- nonimmigrant classification (i.e., F, J, or M) and the date on which a visa was issued or a change to such classification was approved;
- current academic status, including whether the individual is maintaining full-time student status; and
- whether any disciplinary action has been taken against the individual as a result of being convicted of a crime.

The new law adds the following items to the list of data the government must collect from educational institutions:

- student's date and port of entry;
- date of enrollment;
- degree program and field of study; and
- date and reason for termination of enrollment.

Foreign students also will be subject to new reporting requirements when they apply for a visa. The prospective student will be required to provide information about his or her family, contacts, prior work history, and references in the home country.

Compliance Reviews. In addition, the BSA requires DHS, in consultation with the Department of Education, to conduct periodic compliance reviews. The DHS or State Department may terminate, suspend, or limit an educational institution's authorization to receive foreign students if it has failed to comply with the statute's record-keeping and reporting requirements.

Student and Exchange Visitor Information System (SEVIS)

SEVIS is an Internet-based system developed to comply with the foreign student monitoring mandates in the USAP, the BSA, and previous legislation. The system maintains information on nonimmigrant students (F and M visa categories), exchange visitors (J visa categories), and their dependents (F-2, M-2, and J-2 visa categories).

SEVIS enables institutions to transmit electronic information via the Internet to the DHS and State Department throughout a student's or exchange visitor's stay in the United States. The system will reflect changes such as admission at a port of entry, change of address, change in program of study, and other details. SEVIS will also provide system alerts, event notifications, and basic reports to the institutions and DHS field offices. (CIPRIS, the Coordinated Interagency Partnership Regulating International Students, was a pilot program that preceded SEVIS and that tested the concepts associated with new data collection and reporting methods.)

Timing of Implementation. The USAP accelerated the deadline for INS to have SEVIS fully operational to January 1, 2003. INS began implementing SEVIS on a voluntary basis on July 1, 2002. Under a final regulation published on December 11, all institutions had to use SEVIS for F and M nonimmigrant students by January 30, 2003. The State Department set the same deadline for sponsors to use SEVIS for J visa exchange visitors in separate regulations published on December 12. Initially, only data from newly enrolled students must be entered into SEVIS; data for currently enrolled students may be, but need not be, entered. If a currently enrolled student needs a new or modified Form I-20, however, the institution must enter the student's data into SEVIS at that time. Forms I-20 issued prior to February 15, 2003 will be accepted through July 31, 2003.

How SEVIS Works. SEVIS aims to fully automate many paper-based processes currently in place for enrolling students, maintaining data, and transmitting changes of information among educational institutions, the DHS, and the State Department. Form I-20 for F and M nonimmigrant students and Form DS-2019 (previously Form IAP-66) for J nonimmigrant exchange visitors will continue to be used, but creating a Form

I-20 or Form DS-2019 will involve accessing SEVIS via the Internet and entering the information electronically into a central database. Institutions will no longer need to complete and mail multiple copies of forms, nor to maintain paper copies, as records will be accessible electronically through SEVIS. Each SEVIS Form I-20 will contain a SEVIS ID number, which will remain the same as long as the student maintains his or her valid, original nonimmigrant status.

An arriving student will show the SEVIS Form I-20 at the port of entry to the INS inspector, who will record the SEVIS ID number for transmission to SEVIS. If a student is issued multiple SEVIS Forms I-20 from different institutions, SEVIS can link those forms to the individual and cancel SEVIS Forms I-20 from institutions the student decided not to attend. SEVIS will also automatically terminate any Form I-20 that has not been used by the program start date for issuance of a visa or change of status.

Accessing SEVIS requires MS Internet Explorer 5.0 or better or Netscape 4.7 or better. No user fee will be required to access SEVIS. Institutions that opt to use batch capability may need to pay to make their existing systems compatible with SEVIS. Information and announcements about SEVIS is available at http://www.immigration.gov/graphics/services/tempbenefits/sevp.htm or from the SEVIS Help Desk at 1-800-892-4829.

Authorization Required to Use SEVIS. Before an institution may enroll in SEVIS it must be certified or re-certified by INS. INS has implemented a two-stage process for certification review (see July 1 *Federal Register* notice). Phase I, which began on July 1, 2002, and closed on September 25, 2002, was a preliminary enrollment period for certain currently accredited institutions that elected to participate. Eligible institutions that applied during Phase I were granted preliminary access to SEVIS prior to undergoing a full certification review and were not required to pay the certification fee at that time. These institutions will have to undergo a site visit and pay the associated fee prior to May 2004.

On September 25, 2002, INS issued an interim rule implementing Phase II, requiring all institutions not already approved to use SEVIS under Phase I to undergo certification review and to pay the associated fee prior to enrollment in SEVIS. The fee is $580, plus $350 for each additional campus to cover the cost of site visits. To be reviewed and granted access to SEVIS prior to January 30, 2003, INS strongly encouraged institutions to submit an electronic petition for approval (Form I-17) via SEVIS by November 17, 2002. (INS said that it could not guarantee timely final action on any petition for approval not filed by November 17.) An institution with a petition for approval pending after January 30, 2003, will be unable to admit foreign students until approved by INS/DHS and granted access to SEVIS. Additionally, an institution's INS approval to admit foreign students will be withdrawn automatically as of January 31, 2003, if the institution has not submitted a petition for approval by January 30.

Institutions not currently approved by the DHS or the State Department must first obtain a temporary User ID and password (valid for 30 days) by contacting the SEVIS system administrator through the SEVIS Web site listed above. Using the temporary user ID and password to access SEVIS, the institution can complete a Form I-17 petition for approval by the DHS.

The interim rule provides that DHS must approve institutions biennially as required by a presidential directive and the BSA. Previously, an institution's approval continued indefinitely. The INS plans to conduct a separate rulemaking proceeding to implement more specific procedures on applications for biennial certification review. Finally, institutions must update SEVIS to reflect any material modifications in name, address, or curriculum within 21 days of the modification.

Interim Student and Exchange Authentication System (ISEAS)

On September 18, 2002, the Department of State issued an interim rule creating an electronic system known as ISEAS—effective September 11, 2002—to implement certain transitional requirements of the BSA related to monitoring of foreign students and exchange visitors. The BSA required the State Department to establish an interim electronic monitoring program for use until SEVIS was fully operational. State, INS, approved educational institutions, and exchange visitor program sponsors used ISEAS to track foreign students until SEVIS was fully operational. ISEAS was shut down on February 15, 2003.

December 11, 2002, SEVIS Regulations

Reporting Requirements. Under the final regulation, institutions are required to maintain additional information on foreign students, including registration information and information regarding certain events (enrollment, start date, failure to enroll, etc.). Currently, 8 C.F.R. § 214.3(g) requires institutions to maintain certain basic information on the premises but imposes no duty to report such information to INS except when INS issues a request. If a student no longer attends the institution, the institution need report only that fact. With the new system, the information will be accessible by DHS directly through SEVIS; the DHS will not need to issue a request to the institution.

Under the new rules that took effect January 1, 2003, institutions must continue to maintain all information required by 8 C.F.R. § 214.3(g)(1)(iv)-(v) as well as the individual's current address and academic status. The address provided should be where the student physically resides, unless he or she is unable to receive mail at that address (such as some on-campus situations where central mailing addresses are used for students in dormitories). In that case, the institution should report the mailing address but is required to keep in its own records the physical address and provide it to DHS upon request.

Within 30 days after the deadline for registering for classes in each term or session, institutions will be required to report the following registration information:

- whether the student has enrolled, dropped below a full course of study without prior authorization by the institution, or failed to enroll;
- the current address of each enrolled student; and
- the start date of the student's next session, term, semester, trimester, or quarter.

Within 21 days of occurrence, institutions will be required to report these events:

- a student's enrollment at the institution;
- the start date of the student's next term or session;
- a student's failure to enroll;
- a student dropping below a full course of study without prior authorization;
- any other failure to maintain status or complete the program;
- a change of the student's or dependent's legal name or address;
- any disciplinary action taken by the institution against the student as a result of the student being convicted of a crime; and
- a student's graduation prior to the program end date listed on the form.

Student Obligations. The regulations limit the amount of time foreign students may be in the United States prior to the commencement and after completion of the course of studies. F-1 and M-1 students may not enter the United States more than 30 days prior to the beginning of the course of study instead of the current 60-day grace period. F-1 students will have 60 days (and M-1 and J-1 nonimmigrants will have only 30 days) to depart the country—but those grace periods will not apply to individuals who do not complete their program or otherwise fall out of status. If a student is authorized by the designated school official (DSO) to withdraw from classes, the student will have 15 days to make arrangements to leave the country.

Students are required to notify the institution of any change in legal name or home address within 10 days of the change. (The institution must update SEVIS within 21 days of notification.)

Designated School Officials (DSOs). Instead of five DSOs at each institution (or each campus), institutions will now be allowed to have 10, including one "principal designated school official" (PDSO), a newly created position. A provision in the May 16, 2002, proposed regulations to create a three-tiered structure with new "administrative school officials" to handle purely administrative matters was dropped in the final rules. All DSOs must be U.S. citizens or lawful permanent residents. Any changes to the institution's DSOs have to be updated in SEVIS within 21 days of the change.

Distance Education; Online Programs. The regulations limit enrollment of F-1 and M-1 students in distance education courses and online programs because such programs do not require physical presence in the United States. For an F-1

student, no more than one class or three credits per semester of online and distance education credits may be counted toward a "full course of study." No online or distance education courses that do not require the student's physical presence may count toward the full-time course of study of an M-1 student.

Reduced Course Loads. Under the old rules, a student who dropped below a full course of study due to a medical condition could resume a full course load upon recovery. The new regulations greatly restrict this flexibility. An institution may authorize a reduced course load due to a medical condition only if the condition is substantiated by documentation from certain medical professionals, but for no more than one year for an F-1 student and five months for an M-1 student. The only other circumstances under which an institution can authorize a reduced course load for an F-1 student are if the student has academic difficulties related to initial adjustment or if, at the end of the education program, the student does not need to take a full load for completion. In either case, the student may not withdraw from all classes but must take at least six credit hours and must resume full-time status in the next term. M-1 students may drop below full-time status only for medical reasons. Any course-load changes must be reported to SEVIS. A student who drops below a full course of study without prior approval by the DSO is considered out of status.

Student Transfers. The regulations require that the institution to which the student is transferring determine that the student has been in valid status at the prior institution and is eligible to transfer. On notification of the student's intent to transfer, the current institution must update SEVIS with a release date. On the release date, the new institution will be granted full access to the student's SEVIS record (and the old institution will no longer have access) and may issue a new SEVIS Form I-20. The student will be required to report to the new institution within 15 days of the program start date. The transfer is effectuated once the new institution notifies SEVIS, within 30 days, that the student has enrolled in classes.

Practical Training. An F-1 student can pursue up to 12 months of practical training for each program level (undergraduate, graduate, etc.). The student must have been enrolled for at least one full academic year in full-time study at an approved institution. F-1 students may count time spent during study-abroad programs toward the academic year if they studied full-time in the United States for at least one academic term first. An M-1 student must apply for practical training no more than 90 days before the end of their program but prior to completion.

F-1 students may apply for optional practical training (OPT) that is directly related to their field of study as much as 90 days before completing a full academic year of study but may not begin OPT before completing the year. Students must, however, apply for OPT prior to completing their program of study, not within 60 days of completion as is currently allowed. Similarly, M-1 students will have to apply for practical training before completing the program but cannot apply more than 90 days before the program completion date.

Internships With International Organizations. F-1 students who are offered inter-national organization internships must apply for employment authorization at the appropriate DHS service center instead of the local office. Wage-and-labor attestations are no longer required.

Extensions of Student Status. Under the new rules, an F-1 or M-1 visa holder must be in current lawful status to apply for an extension. Extensions of F-1 status do not require adjudication by INS. Instead, DSOs may grant extensions of stay through SEVIS by updating the program end date and issuing a new SEVIS Form I-20, thus eliminating the need to submit Form I-538 as previously required. F-1 students may apply for a program extension at any point before the program end date listed on the Form I-20 instead of only within 30 days of the program end date. The DSO must certify that the student has continually maintained status and that the delays in completion are due to compelling academic or medical reasons. The regulation also eliminates the DSO's ability to add a one-year grace period to the amount of time that the DSO estimates the F-1 student will need to complete the program. Instead, the DSO must set the completion date based on the time an average student (not an average foreign student, as currently provided) would require to complete the program.

An M-1 student will have to file a Form I-539 with the appropriate DHS Service Center to request approval for an extension at least 15 days, but no

more than 60 days, from the program end date on the student's I-20. DSOs must update SEVIS, recommending the extension, and print it for submission by mail to the DHS with the I-539. M-1 students have to show a compelling academic or medical reason for the delay in completing the program. Although prior rules did not limit the number of M-1 extensions permitted, the new regulations restrict the cumulative time of M-1 extensions to three years from the student's original start date, plus 30 days.

Eligibility for Reinstatement of Student Status. In the past, F-1 and M-1 students could apply for reinstatement of student status with no specified time limit for being out of status. Under the new rules, F-1 and M-1 students must apply to the DHS for reinstatement within five months of being out of status, and the circumstances under which reinstatement is allowed are restricted.

Dependents. SEVIS will link information about dependents to the primary nonimmigrant. Each dependent must have his or her own I-20, issued by the institution, although before August 1, 2003, dependents will be allowed to enter the country with a copy of the F-1 or M-1 student's I-20 if exigent circumstances are demonstrated.

The regulations prohibit full-time study by F-2 and M-2 spouses and restrict such study by F-2 and M-2 children but does allow them to enroll in vocational or recreational courses. A spouse or child who wishes to study full-time should apply for a change to F-1, J-1, or M-1 status. A spouse or child who began full-time study prior to January 1, 2003, is allowed to continue but had to file for a change in classification by March 11.

Commuter Status for Part-Time Students

On November 2, 2002, Congress amended the Immigration and Nationality Act to establish two new visa classifications, F-3 and M-3, for citizens of Canada and Mexico who commute to approved institutions in the United States. These students may be either full- or part-time and are subject to the same reporting requirements and SEVIS processes as F-1 or M-1 students. Family members of F-3 and M-3 students are not eligible for dependent visas.

Information Technology Officials and Officials Who Process Subpoenas and Warrants

As providers of communication services—including telephones, computers, and Internet access—colleges and universities are affected by Title II of the USA Patriot Act (USAP), Enhanced Surveillance Procedures. Many Title II provisions will sunset—that is, cease to have effect unless renewed by Congress—on December 31, 2005.

Stored Voicemail and E-mail Messages. As with e-mail messages, stored voicemail messages less than six months old may be seized with a search warrant rather than a wiretap order.

Required Disclosure of Electronic Communications or Records. An electronic service provider may be subpoenaed to disclose additional basic subscriber information, including local and long-distance telephone connection records, records of session times and durations, telephone or instrument number or other subscriber number or identity, temporarily assigned network address, and means and source of payment.

Pen/Trap Orders. To cover the Internet, a so-called "pen register" or "trap and trace" device may lawfully be used to obtain dialing, routing, addressing, or signaling information transmitted by wire or electronic communication if such information does not include communication content. A federal court can authorize a pen/trap order applicable to any wire or electronic service provider in the United States whose assistance may facilitate execution of the order and the order is not required to identify all parties to whom it applies.

Internet Surveillance. Government officials may also install certain devices, such as "Carnivore"—now known as DCS 1000—to track Internet use. Carnivore was the controversial program sponsored by the Federal Bureau of Investigation (FBI) that enabled government criminal investigators to intercept and collect information on the Internet. The USAP as passed, unlike earlier versions, imposes on service providers no new obligation to furnish facilities or technical assistance to aid law enforcement in this regard and authorizes compensation for reasonable expenditures incurred in providing such aid.

Compelled Disclosure of "Any Tangible Things." To protect against international terrorism or clandestine intelligence activities, the FBI can obtain an order to compel any entity to release "any tangible things." The USAP prohibits any person from disclosing (other than to individuals necessary to produce the records) that the FBI sought or obtained such records.

Voluntary Disclosure of Electronic Communications or Records. Providers of "electronic communication to the public" may, without subscriber/customer consent, voluntarily disclose to law enforcement the contents of a subscriber's/customer's electronic communications and non-content information if the provider "reasonably believes" that immediate danger of death or serious injury to any person requires disclosure.

Computer Trespassers. In some circumstances, providers may permit law enforcement officials and individuals acting for them to intercept, without a warrant, communications of *computer trespassers* (individuals who access protected computers without authorization). A person who has an "existing contractual relationship with the owner or operator of the computer for access to all or part of the protected computer" is not a computer trespasser. There is no express immunity for a computer trespass victim who enlists law enforcement assistance.

Computer Hacking. The USAP increases penalties for certain computer-hacking crimes, including accessing and transmitting destructive programs such as viruses to computers. If the loss exceeds $5,000—for example, if the hacker damaged university equipment—the hacker may be sued.

Nationwide Search Warrants. In terrorism investigations, search warrants may be issued with nationwide effect by a court in any district of the United States in which activities related to terrorism may have occurred. Any court having jurisdiction over an offense under investigation may issue a search warrant for unopened e-mail or voice-mail messages that are less than six months old.

Court Order for Education Records. The USAP amends FERPA to permit non-consensual disclosure of education records that law enforcement officials consider relevant to a terrorism investigation.

Information technology officials and those who process subpoenas and warrants should know how the USAP enhances law enforcement's powers to investigate and combat terrorism, including through surveillance, computer-related searches and seizures, electronic evidence gathering, and voluntary disclosure of information by institutions that provide certain communication services. The following chart summarizes these changes in the law from the perspective of a recipient of a law enforcement request.

USA Patriot Act: Law Enforcement Requests

New Requirements Under USA Patriot Act	Analysis	Prior Law
Stored voicemail messages that are less than six months old may be seized with a search warrant.	Consistent with law regarding stored e-mail messages that are less than six months old, a search warrant—not a wiretap order—may be used to order disclosure of stored voicemail messages that are less than six months old.	A wiretap order is required to seize unopened voicemail messages that are less than six months old (but a search warrant can be used to seize stored e-mail messages that are less than six months old).
Any court having jurisdiction over the offense under investigation may issue a search warrant for unopened e-mail or voicemail messages that are less than six months old.	An institution may receive a search warrant for unopened e-mail or voicemail messages that are less than six months old from a court *outside* its state or federal judicial district.	A search warrant for unopened e-mail messages that are less than six months old must be issued by a court in the jurisdiction where the provider is located.
The basic subscriber information that law enforcement may subpoena from an electronic service provider includes local and long-distance telephone connection records, records of session times and durations, telephone or instrument number or other subscriber number or identity, temporarily assigned network address, and means and source of payment.	A wide array of basic subscriber information may be requested with a subpoena.	Law enforcement can use a subpoena to compel an electronic service provider to disclose certain basic subscriber information.
A so-called "pen register" or "trap and trace device" (pen/trap) order can be used in connection with communication technologies other than telephones and can require software to intercept the information.	A pen/trap order may require use of software to intercept non-content information related to the Internet and other computer network services.	It is unclear whether a pen/trap order applies to communication technologies other than telephones and to interception mechanisms other than physical devices.
A federal court can authorize a pen/trap order applicable to any wire or electronic service provider in the United States whose assistance may facilitate execution of the order and the order is not required to identify all parties to whom it applies.	An institution may receive a pen/trap order issued by a court *outside* its state or federal judicial district. If the institution is not identified in the order, it may request certification that the order applies to it.	A court can authorize installation and use of a pen/trap device only within its jurisdiction.

New Requirements Under USA Patriot Act	Analysis	Prior Law
To protect against international terrorism or clandestine intelligence activities, the Federal Bureau of Investigation (FBI) can obtain an *ex parte* order to compel *any* entity to release "*any* tangible things."	An *ex parte* order may be used to compel disclosure of business records or other tangible items—for example, hard drives or student records. The order need not disclose the purposes for which it is issued and the institution may not disclose (other than to individuals necessary to produce the items) that the FBI sought or obtained the items.	The FBI can obtain an *ex parte* order to compel certain businesses to disclose business records in connection with foreign intelligence and international terrorism investigations.
Providers of electronic communication to the public* may, without subscriber/customer consent, voluntarily disclose to law enforcement the contents of a subscriber's/customer's electronic communications and non-content information if the provider "reasonably believes" that "immediate danger of death or serious injury to any person" requires disclosure. *Whether a particular institution's computer operations constitute provision of electronic communication to the public is a legal and factual question.	A provider of electronic communication to the public may disclose to law enforcement subscriber/customer electronic communications and non-content information without consent or legal process in emergency situations, such as a terrorist threat.	Providers of electronic communication to the public can voluntarily disclose to law enforcement the contents of a subscriber's or customer's electronic communications if, among other circumstances: (1) the contents were inadvertently obtained by the provider and appear to pertain to the commission of a crime, or (2) if necessary for the provider to protect its rights or property.
A computer-trespass victim may request law enforcement to monitor a computer trespasser, but there is no express immunity for a computer-trespass victim who enlists law enforcement assistance.	An institution may seek law enforcement assistance in connection with monitoring hackers but may be liable if the action is unlawful.	It is unclear whether federal law permits a hacker victim to obtain law enforcement assistance in monitoring a computer trespasser.
In terrorism investigations, search warrants may be issued with nationwide effect by a court in any district of the United States in which activities related to terrorism may have occurred.	An institution may receive a search warrant from a court *outside* its state or federal judicial district.	Search warrants must be issued by a court in the district where the place to be searched or thing to be seized is located.
FERPA does not forbid an institution to disclose education records to the Attorney General or his or her designee without student consent in response to an *ex parte* order related to the investigation or prosecution of terrorism crimes. In connection with such an order, an institution need not comply with FERPA record-keeping requirements and is not "liable to any person" for good faith disclosure.	Without violating FERPA, institutions may disclose education records to the Attorney General or his or her designee in response to an *ex parte* order related to a terrorism investigation. Unlike other non-consensual disclosures permitted under FERPA, an institution is immune from liability for good faith disclosure in connection with such orders.	With limited exceptions, including exceptions relevant to anti-terrorism activities, FERPA forbids institutions to release education records or personally identifiable information contained in such records to any individual, agency, or organization without the student's written consent.

Research Administrators and Environmental Health and Safety Officers

Both the USA Patriot Act (USAP) and the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (BPRA) include new provisions that regulate possession, use, and transfer of certain dangerous biological materials and other toxins defined as "select agents". These include anthrax, smallpox, and other pathogens. A significant portion of the facilities reporting possession of select agents are academic institutions.

The new requirements are much broader than existing Department of Health and Human Services (HHS) rules, promulgated in 1997, that regulate the transfer of select agents. Now, the possession and use of select agents will be strictly regulated, with requirements for registration, security risk assessments, safety and security plans, training, record keeping, inspections, and notifications.

Under BPRA, HHS is responsible for regulating to protect public health and safety and the Department of Agriculture (USDA) is responsible for regulating biological agents and toxins to protect animal and plant health, and animal and plant products. The two agencies have separate lists of covered agents and toxins, with some appearing on an "overlap" list that are regulated by both agencies. The discussion below focuses on the regulations issued by the Centers for Disease Control and Prevention (CDC), a component of HHS. USDA regulations are quite similar, with equivalent deadlines.

The USAP was first to address the need to increase security for dangerous biological agents. The USAP punishes by fine and/or up to 10 years of imprisonment for knowing possession of a dangerous biological agent, toxin, or delivery system of a type or in a quantity not "reasonably justified" by a prophylactic, protective bona fide research or other "peaceful purpose." Further, nationals of countries determined to support terrorism, individuals indicted for or convicted of serious crimes, and certain others are prohibited to possess, receive, or transport a select agent. BPRA, enacted in June 2002, addressed safeguards for select agents in much greater detail.

Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (BPRA)

Overview of Requirements. The BPRA includes detailed new requirements applicable to *select agents* and strict timelines for implementation.

- Requirements include new standards and enforcement procedures for possession, use, and transfer of select agents, including required training of laboratory personnel and establishing safety and security procedures for laboratories.
- Access to select agents is limited to individuals with a legitimate "need." HHS has new authority to conduct inspections to ensure compliance.
- Names of individuals who need access to select agents must be disclosed to the Department of Justice for approval.
- By September 10, 2002, facilities were required to notify HHS of the select agents in their possession or that the institution did not possess any select agents.
- The select agent list will be revised by HHS (specifically, the CDC) at least biennially.
- All facilities with select agents will be required to register with HHS.
- Knowing possession without registration, or transferring a select agent to an unregistered facility, is a crime.

As a first step, BPRA required facilities, including universities and colleges, in possession of "select agents" to notify HHS or USDA—or both agencies, depending on the materials present—no later than September 10, 2002. On August 6, 2002, the CDC published a "Notice of Approval of Data Collection," an accompanying guidance document, and notification form. The notification form listed the select agents and high-consequence pathogens and toxins to be reported. Almost 200,000 facilities were mailed official reporting forms in late August that needed to be returned naming a responsible facility officer, and indicating any select agents on site, or that the facility did not possess any such agents.

A chart that compares the provisions of BPRA relating to handling, use, and transportation of select agents and toxins to previous law is available on the ACE Web site at http://www.acenet.edu/washington/letters/2002/06june/biohazard.chart.cfm.

December 13, 2002, Interim Final Regulations

BPRA gave HHS and USDA 180 days after enactment to issue interim final regulations implementing the provisions on select agents and toxins. The agencies each published regulations on December 13, 2002, with similar requirements and implementation schedules. As interim final rules, they took effect on February 7, 2003, even though comments were solicited by February 11.

The agencies will issue final rules at a later date. The following summarizes the key provisions of the interim final regulations issued by the CDC under 42 CFR Part 73.

List of Select Agents. The regulations provide a list of the regulated agents and toxins, developed after consideration of comments received in response to a preliminary list published on August 23, 2002. BPRA provided that the following criteria be considered:

- the effect on human health of exposure to the agent or toxin;
- the degree of contagiousness and the methods by which the agent or toxin is transferred to humans;
- the availability and effectiveness of treatments and immunizations; and
- any other criteria, including vulnerability of special populations that the secretary of HHS considers appropriate.

More than 40 agents are included in the list in the interim final regulation, categorized as viruses, bacteria, fungi, toxins, and genetic/recombinant elements. There are some circumstances under which exemptions may be granted.

Registration of Entities. Under BPRA, all entities, including colleges and universities, that possess, use, receive, or transfer any select agents or toxins must apply for and receive a certificate of registration from HHS or USDA. The regulations set forth the information that must be included in the application as follows:

- identification information;
- name, source, characterization, and quantities held of all select agents and toxins included in the registration;
- location, including building, room, and floor plan, for each place that select agents will be stored or used;
- information addressing safety, security, emergency response plans, and training;
- name, position, and identification information regarding the responsible official; and
- a list of individuals who will need access to the select agents and toxins.

Application forms are available on the CDC Select Agent Program Web site at www.cdc.gov/od/sap.

The registration will only be valid for the specific agents, locations, individuals, and activities covered in the application. The Responsible Official must report any changes to the information submitted in the application promptly and must apply for an amendment to the certificate of registration.

Security Risk Assessments. The regulations require that the entity, the responsible official, any individual who "owns or controls the entity," and any individuals who will have access to select agents or toxins be approved by HHS or USDA based on a security risk assessment by the U.S. Attorney General. The security risk assessment will evaluate whether the person is a restricted person under the USAP (including, for example, foreign nationals from countries that are on the State Department's list of state sponsors of terrorism, or individuals who have been indicted or convicted of a crime punishable by a prison term exceeding one year).

Under the implementation schedule in the interim regulations, institutions had to submit applications for risk assessments of the entity, the entity's owner and the responsible official(s) by March 12 and must submit applications for other individuals by April 12. The application, FBI form FD-961, was posted on the web on March 12. The form indicates that academic institutions do not need to provide information about "individuals who own or control the entity." Instructions on submission of fingerprints are forthcoming.

Responsible Official. The institution must designate an individual to act as the responsible official. He or she must be familiar with the requirements of the regulations and have authority and responsibility to ensure that they are met on behalf of the institution. The responsible official may identify one or more alternate responsible officials who may serve in his or her place. The CDC recommends that the responsible official and alternates be safety officers or senior management officials but that they not be individuals who are engaged directly in work with select agents.

Safety, Security, and Emergency Response Plans. Any entity registered to use select agents must develop and implement a safety plan to ensure that safety provisions are commensurate

with the risk associated with the agents or toxins used. The requirements are tied to existing CDC and National Institute of Health standards classified for biosafety levels 1 through 4. Institutions should, for the most part, already be complying with these standards. Similarly, institutions possessing select agents are likely to already have emergency response plans in place that comply with the Occupational Safety and Health Administration (OSHA) standards and other environmental protection laws and will only need to ensure that specific provisions relating to select agents and toxins are appropriate. The requirements in the interim regulations for safety and emergency response plans took effect on February 7, 2003, when the new rules became effective.

Institutions will have more time to develop and implement their security plans, however. Under the phased approach adopted by the agencies, security plans must be developed by June 12, 2003, and implemented by September 12. The institution's security plan must establish policy and procedures to ensure security of areas containing select agents. According to the regulations, institutions must use a systematic approach to define threats, examine vulnerabilities, and mitigate risks. The rules delineate a number of specific areas that must be addressed including physical security and access control, minimum qualifications of individuals, inventory control, and reporting. In addition, for areas containing select agents, the rules include specific provisions that must be included, such as requiring:

- personnel not approved for access to select agents who are performing routine cleaning, maintenance, and so forth, to be escorted by an approved person at all times;
- storage areas for select agents to be locked when not in direct view of approved staff and monitored in other ways, such as video surveillance, as needed; and
- inspection of all packages upon entry and exit from the area.

Training and Record Keeping. Institutions are required to provide training to all individuals who work with select agents or in areas where they are stored and must keep records of the training. There is a provision allowing the responsible official to certify that individuals already working with select agents have sufficient knowledge and skills to safely carry out their duties. Under the phased-in implementation schedule, training on the security plan does not have to be completed until September 12, 2003.

The regulations include detailed record-keeping requirements. Institutions must maintain accurate records on:

- individuals approved for access to select agents and toxins;
- inventory of each select agent held, including quantities held, used, transferred, or destroyed;
- individuals who have accessed select agents, quantities taken and returned, and applicable dates; and
- individuals who accessed an area where select agents are used or stored.

For More Information

Colleges and universities face many challenges to meet increased security needs for their campuses, comply with a myriad of new and changing laws and regulations, and address concerns of their students. ACE, NACUBO, and the other higher education associations are working together in Washington to represent the interests of their members in the legislative and rule-making processes and to keep institutional administrators informed of new requirements that will affect colleges and universities.

ACE and NACUBO will from time to time provide updates on new developments on our Web sites. However, institutions, to meet their varying and specific needs, are well advised to consult their counsel as issues in these sensitive areas arise. Links to Web sites listed throughout this report are provided below, along with several other sites that provide additional resources.

For questions or additional information: At NACUBO, contact Anne Gross, assistant vice president, business and regulatory affairs, by telephone at 202-861-2544 or by e-mail at anne.gross@nacubo.org.

At ACE, contact Sheldon E. Steinbach, vice president and general counsel, by telephone at 202-935-9361 or by e-mail at Sheldon_Steinbach@ace.nche.edu.

Web Resources

American Council on Education www.acenet.edu

NACUBO www.nacubo.org/public_policy

USA Patriot Act – Privacy Issues

U.S. Department of Education, on FERPA
http://www.ed.gov/offices/OM/fpco/hot_topics.html

American Library Association
http://www.ala.org/washoff/#hsb

Electronic Privacy Information Center
http://www.epic.org/privacy/terrorism/usapatriot/

Nonresident Aliens, SEVIS Issues

U.S. Department of Homeland Security
www.immigration.gov/graphics/services/tempbenefits/sevp.htm

NASFA: the Association of International Educators http://www.nafsa.org/

Bioterrorism/Select Agent Issues

Centers for Disease Control www.cdc.gov/od/sap

American Society for Microbiology
http://www.asm.org/pasrc/bioprep.htm

Glossary of Acronyms

AEDPA: Antiterrorism and Effective Death Penalty Act of 1996. Created a "select agent" list and prohibited transfers of select agents, with certain exceptions, unless to registered facilities.

BSA: Border Security Act, or Enhanced Border Security and Visa Entry Reform Act of 2002. Addresses monitoring of and data collection regarding foreign students, including establishment of an Internet-based information system.

BPRA: Health Security and Bioterrorism Preparedness and Response Act of 2002. Spurs development of new therapeutic products to combat bioterrorism, strengthens federal oversight of biological agents and toxins, and establishes new management goals for the Food and Drug Administration that will have a major impact on drug and biological product approval.

CIPRIS: Coordinated Interagency Partnership Regulating International Students was a pilot program that preceded SEVIS and tested the concepts associated with new data collection and reporting methods.

DSO: Designated School Official. Under the rules implementing SEVIS, each institution may have up to 10 DSOs with access to SEVIS to provide data on foreign students.

FERPA: Family Educational Rights and Privacy Act. Requires educational institutions that receive funds under a program administered by the U.S. Secretary of Education, such as a federal student financial aid program, to comply with certain policies regarding student education records, including policies related to disclosure of such records.

IIRIRA: Illegal Immigration Reform and Immigrant Responsibility Act of 1996. Included criminal penalties for immigration-related offenses, authorization for increases in enforcement personnel and enhances enforcement authority. IIRIRA called upon the INS to develop an electronic system for collecting and tracking visitors coming to the U.S. on F,J, or M visas. (the initial tracking system, CIPRIS).

ISEAS: Interim Student and Exchange Authentication System. A temporary system operated by the Department of State that implemented certain transitional requirements of the Border Security Act (BSA) related to monitoring of foreign students and exchange visitors until the Student and Exchange Visitor Information System (SEVIS) became fully operational.

SEVIS: Student and Exchange Visitor Information System. An Internet-based system developed to comply with the foreign student monitoring mandates in the USA Patriot Act, the Border Security Act, and previous legislation. The system maintains information on nonimmigrant students (F and M visa categories), exchange visitors (J visa categories), and their dependents (F-2, M-2, and J-2 visa categories), and enables institutions to transmit electronic information via the Internet to the INS and State Department throughout a student's or exchange visitor's stay in the United States.

USAP: USA Patriot Act, or Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. Enhances the power of law enforcement to combat terrorism through surveillance and other information-gathering techniques and lays the groundwork for subsequent immigration and bioterrorism legislation.