THE WAR ON TERRORISM AFFECTS THE ACADEMY: PRINCIPAL POST-SEPTEMBER 11, 2001 FEDERAL ANTI-TERRORISM STATUTES, REGULATIONS AND POLICIES THAT APPLY TO COLLEGES AND UNIVERSITIES

JAMIE LEWIS KEITH*

I. INTRODUCTION

The United States is waging its "war on terrorism,"[1] borne of the hideous attacks of September 11, 2001, in many sectors throughout our country, including academia. Over the last two and a half years, several significant federal laws and government policies have brought detailed and prescriptive requirements into research laboratories, student life, admissions and counseling offices, international scholars' and students' offices, sponsored research offices, and basic contracts and administrative processes of colleges and universities across the United States. These laws, and the regulations that implement them, represent a decided emphasis on law enforcement and terrorism prevention and a decided departure from the previously prevailing emphasis on safety in research and reasonable controls to prevent accidental or unintentional adverse effects. In many respects, these new laws, regulations, and policies challenge deeply held values and long-standing

* Senior Counsel, Massachusetts Institute of Technology; also Managing Director for Environmental Programs and Risk Management of MIT. This article represents the personal work of Ms. Keith, and does not represent the views of MIT or Ms. Keith's legal advice to MIT or to the reader. The general legal analysis in this article may change in the context of particular facts and circumstances. The author is indebted to Jeffrey Swope, Esq., and George Olson, Esq., of Palmer & Dodge for their peer review of this article and consultation, and to Richard Johnson, John Barker, Ronald Lee, and Gregory Levine of Arnold & Porter for their peer review and consultation on Part VI of this article and notes 30 and 160. The author thanks Ms. Claudia Molina of Arnold & Porter for her cite checking.

1. *See* President George W. Bush, 2002 State of the Union Address (Jan. 29, 2002), *available at* http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html ("our nation is at war [and] we are winning the war on terror"); President George W. Bush, 2003 State of the Union Address, Jan. 28, 2003, *available at* http://www.whitehouse.gov/news/release/2003/01/print/20030128-19.html ("The war [on terrorism] goes on, and we are winning."). *See also* President George W. Bush's signing letters on the enactment of the USA PATRIOT Act on October 26, 2001, and the Public Health Security and Bioterrorism Preparedness Act of 2002 on June 12, 2002.

practices of American academic culture, such as the open and free exchange of information, the intellectual stimulation of and commitment to a diverse and international campus community, and the culture of inclusion. In some cases, the new laws and policies substitute the judgment of law enforcement for that of educational institutions on matters affecting our core academic and research functions. While most of the laws do not directly restrict the sharing of information in academia, these laws can have the effect of restricting information sharing and some of these laws restrict, or have the effect of restricting, participation in research.[2] If not implemented with wisdom, balance, and care by a knowledgeable academic community and government, these laws, regulations, and governmental policies could seriously threaten the nation's leadership position in higher education, in scientific research, innovation, and advancement, and in the world's economy.[3]

Academia must work in good faith with the federal government to find the right balance between guarding our national security and maintaining the foundations that make our nation great. U.S. academic institutions take seriously their national citizenship and responsibility to aid in our nation's defense against terrorists, whether through our research or through cooperation with legitimate law enforcement efforts to secure our citizens. The challenge for many institutions is how to satisfy the requirements and spirit of the laws without losing the vitality, diversity, and intellectual freedom that are inherent strengths of our academic institutions and are the foundations of our nation.[4]

2. Export controls, addressed *infra* in Part VI, restrict the sharing of information in research (as well as the transfer of equipment, software and technology) under certain circumstances, while the USA PATRIOT Act's bioterrorism provisions, addressed *infra* in Part II, and the Public Health Security and Bioterrorism Prevention and Response Act of 2002, addressed *infra* in Part III, focus on regulating who may participate in certain types of research and the physical and other security controls on how certain research is conducted.

3. *See* Albert H. Teich, *Will Science Become Another Victim of 9-11?* (Mar. 6, 2003), *available at* http://www.potomacinstitute.org/pubs/Teich030603.pdf. *See also infra* note 5.

4. *See* MIT Ad Hoc Faculty Committee on Access to and Disclosure of Scientific Information, *In the Public Interest* (Jun. 12, 2002), *available at* http://web.mit.edu/faculty/reports/publicinterest.pdf [hereinafter MIT Ad Hoc Faculty Committee]; Genevieve J. Knezo, Congressional Research Service, The Library of Congress, *Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education* (Apr. 8, 2002), *available at* http://www.aau.edu/research/csterror.pdf; Association of American Universities, *AAU Survey on International Students and Scholars* (Nov. 14, 2002), *available at* http://www.aau.edu/resources/visa.pdf. Some institutions, and the professional organizations that represent them, have begun to advocate for collaboration between government and the academy in order to find the right balance for the long and short term welfare of our national economy, security and society. *See, e.g.,* Charles M. Vest, *MIT Report of the President for Academic Year 2001-2002, Response and Responsibility, Balancing Security and Openness in Research and Education, available at* http://web.mit.edu/president/communications/rpt01-02.html (last visited Apr. 4, 2004); Dana A. Shea, Congressional Research Service, The Library of Congress, *Balancing Scientific Publication and National Security Concerns: Issues of Congress* (July 9, 2003), *available at* http://www.fas.org/irp/crs/RL31695.pdf; Alice P. Gast, Vice President for Research and Associate Provost, Massachusetts Institute of Technology, *The Impact of Restricting Information Access on Science and Technology, available at* http://web.mit.edu/nobel-lectures/impact.pdf (last visited Apr. 4, 2004).

This article will explore the collective effects on academia of some of the most important post-September 11 anti-terrorism laws and government policies by analyzing the requirements of key provisions of each of them, and by observing the associated changes to campus life and work. The article will focus on bioterrorism prevention laws, export controls, and privacy of student education records. The article will also briefly address the expansion of federal law enforcement investigatory powers and refer to sources of additional analysis of these developments. In addition, this article offers suggestions on how to approach implementation effectively in order to avoid the most undesirable results while complying with the new legal requirements.

II. BIOTERRORISM PROVISIONS OF THE USA PATRIOT ACT

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act")[5] was enacted by Congress and signed into law by President Bush on October 26, 2001, shortly after the terrorist attacks of September 11, 2001. This Act is aimed at preventing and combating terrorism against the United States and affects a broad range of activities at academic institutions, from activities involving biological agents and toxins,[6] to interactions with law enforcement officials conducting certain foreign intelligence and criminal investigations under expanded investigatory powers,[7] to certain financial activities,[8] to the ease with which federal law enforcement can obtain student "education records" under the Family Education Rights and Privacy Act ("FERPA"),[9] and to the consequences of computer system trespasses for student and other computer "hackers."[10] With

5. Pub. L. No. 107-56, 115 Stat. 272 (2001) (to be codified in scattered sections of 5, 8, 12, 15, 18, 20, 21, 22, 28, 31, 42, 47, 49, 50 U.S.C.) [hereinafter USA PATRIOT Act].

6. *Id.* § 817, 115 Stat. at 385–86 (codified at 18 U.S.C.A. § 175 (2000 & West Supp. 2003); § 175b (West Supp. 2003)) (strengthening criminal laws against biological terrorism). *See infra* Parts II, III, VI.

7. See Title II of the USA PATRIOT Act (expanding federal law enforcement surveillance and other investigatory powers and enhancing the ability of law enforcement and intelligence agencies to share both criminal investigatory and intelligence information). USA PATRIOT Act §§ 201–225, 115 Stat. at 278–96 (codified at scattered sections of 18, 22, 28, 47, 50 U.S.C.A.). *See infra* Part V.

8. See Title III of the USA PATRIOT Act (expanding regulation of banking and other financial institutions to prevent their participation in money laundering). USA PATRIOT Act §§ 301–377, 115 Stat. at 296–342 (codified at scattered sections of 12, 15, 18, 21, 28, 31 U.S.C.A.).

9. Pub. L. No. 93-380, 88 Stat. 571 (1974) (codified as amended at 20 U.S.C.A. § 1232g (2000 & West Supp. 2003)) [hereinafter FERPA]; 34 C.F.R. § 99 (2003); USA PATRIOT Act § 507, 115 Stat. at 367 (codified at 20 U.S.C.A. § 1232g) (amending FERPA to provide for an *ex parte* court order on a certification by a federal employee "in a position no lower than Assistant Attorney General, designated by the Attorney General" to authorize the disclosure of individually identifiable information about a student without the prior consent of the student in certain circumstances). *See infra* Part IV.

10. USA PATRIOT Act § 202, 115 Stat. at 278 (codified at 18 U.S.C.A. § 2516 (2000 & West Supp. 2003)) (adding certain cyber crimes to the list of crimes for which a federal court may issue an order allowing federal law enforcement to listen to telephone or in-person conversations with the approval of the application by a Deputy Assistant Attorney General or higher official in

limited exceptions, Title II of the Act, expanding federal law enforcement's investigatory powers, sunsets on December 31, 2005.[11] Although other Titles of

the Justice Department to the court under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2522 (2000)); USA PATRIOT Act § 217, 115 Stat. at 290–91 (codified at 18 U.S.C.A. §§ 2510, 2511 (2000 & West 2003)) (providing for computer trespasser communications to be intercepted without a court order under the US Criminal Code, 18 U.S.C. § 2511(2) (2000)); Charles Doyle, *The USA PATRIOT Act: A Legal Analysis,* CRS Report for Congress (Order Code RL31377) (Apr. 15, 2002), 2–4, 8, notes 8–9, *available at* http://www.fas.org/irp/crs/RL31377.pdf; and *infra* Part V.I.

11. The following sections of Title II of the USA PATRIOT Act will *not* sunset: § 203(a), 115 Stat. at 278–79 (codified at 18 U.S.C.A. FED. R. CRIM. P. 6(e)(3)(D) (1986 & West Supp. 2003)) (amending FED. R. CRIM. P. 6(e)(3)(D) which is derived from Section 203(a) and authorizes sharing of grand jury information relating to foreign intelligence among certain federal law enforcement, immigration and intelligence agencies, with notice to the federal court of the fact and recipients of the disclosure within a reasonable time after the disclosure); § 203(c), 115 Stat. at 280–81 (codified at 18 U.S.C.A. § 2517(6) (2000 & West Supp. 2003)) (requiring the U.S. Attorney General to create procedures under FED. R. CRIM. P. 6(e)(3)(D) and Title III of the Omnibus Crime Control and Safe Street Act of 1968, 18 U.S.C. 2517(6), for sharing grand jury information relating to foreign intelligence among federal law enforcement, immigration and intelligence agencies when the shared information identifies a "United States person" as defined under the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 ("FISA")); § 205, 115 Stat. at 281–82 (not codified, but published as 28 U.S.C.A. § 532 note (1993 & West Supp. 2003)) (concerning the FBI's employment of translators in connection with counter-terrorism investigations and activities); § 208, 115 Stat. at 203 (codified at 50 U.S.C.A. § 1803 (2003)) (amending Section 103(a) of FISA (a federal law allowing telephone and electronic (e-mail) surveillance, physical searches, pen registers and trap and trace devices and access to items by federal officials to obtain foreign intelligence information upon the issuance of a FISA court order or warrant authorizing such surveillance or search) to increase the number of FISA court judges from seven to eleven and to require at least three of such judges to reside within twenty miles of the District of Columbia, apparently anticipating an increase in requests for such orders); § 210, 115 Stat. at 283 (codified at 18 U.S.C.A. § 2703 (2000 & West Supp. 2003)) (expanding the scope of government access by warrant, court order, or subpoena to telephone and electronic (e-mail) customer or subscriber service records, but not content, without notice to the customer or subscriber, under the U.S. Criminal Code, 18 U.S.C. § 2703(c)(2) from only the customer's or subscriber's name, address, local and long distance telephone billing records, telephone number or other number or identity, and type and length of service, to the subscriber's name; address; local and long distance telephone connection records and records of session times and durations; length of service (including start date); telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit or bank account number)); § 211, 115 Stat. at 283–84 (codified at 47 U.S.C.A. § 551 (2001 & West Supp. 2003)) (clarifying the scope of the Communications Act of 1934, 47 U.S.C. § 551 which governs cable companies, by providing (a) that disclosure to federal law enforcement of subscriber video programming selection records (e.g., cable television) is subject to the Communications Act's more stringent requirements, and (b) that disclosure to federal law enforcement of telephone, e-mail and other electronic records held by cable companies is subject to the less stringent provisions of the U.S. Criminal Code, 18 U.S.C. §§ 2701–2709; *see infra* Part V.2, note 334; Doyle, *supra* note 10, at 6–8); § 213, 115 Stat. at 285–86 (codified at 18 U.S.C.A. § 3103a (2000 & West Supp. 2003)) (amending 18 U.S.C. § 3103a, a supplement to FED. R. CRIM. P. 41(b), to allow a court that issues a warrant or related court order for searches and seizures in order to obtain evidence of an offense constituting a crime under federal law, to authorize delaying any notice required under the Federal Rules or "any other rule of law" in connection with the execution of the warrant or court order if notice "may have an adverse result," provided that notice is given within a reasonable time); § 216, 115 Stat. at 288–89 (codified at 18 U.S.C.A. § 3123(a) (2000 & West Supp. 2003)) (amending 18

the Act do not sunset, efforts to amend Title II, as well as other provisions of the USA PATRIOT Act, are expected as this date approaches. This article addresses the USA PATRIOT Act's provisions relating to biological agents and toxins, the privacy of student education records, and, to some extent, expanded federal law enforcement investigatory powers. Other articles appearing in this Symposium will address the USA PATRIOT Act's provisions relating to the enhanced regulation of non-immigrant foreign citizens in the United States and money laundering.[12]

A. All Biological Agents and Toxins, and Their Delivery Systems

Section 817(1) of the USA PATRIOT Act amends Chapter 10 of Title 18 of the United States Code (the "U.S. Criminal Code") to criminalize a greater range of activities involving biological agents and toxins and the equipment that may be

U.S.C. § 3123(a), to allow any federal court with jurisdiction over the crime being investigated to issue an *ex parte* order authorizing installation of a pen register or trap and trace device (which traces the parties and existence of electronic communications such as e-mail, but does not capture the content of such communications) anywhere in the United States when certain senior Justice Department attorneys apply and the court finds that the "information likely to be obtained . . . is relevant to an ongoing criminal investigation," giving federal courts nationwide jurisdiction for issuing any such order, making any such order applicable to any entities that provide wire or electronic communication service in the United States (without greater specificity), and requiring any such entity to assist federal law enforcement in the execution of such order, and providing for a federal court to issue an *ex parte* order authorizing pen register or trap and trace devices to be installed upon certification of a State law enforcement or investigative officer within the court's jurisdiction); § 219, 115 Stat. at 291 (codified at 18 U.S.C.A. FED. R. CRIM. P. 41(a) (2000 & West. Supp. 2003)) (amending FED. R. CRIM. P. 41(a) to allow the issuance of a search warrant in an investigation of domestic or international terrorism (as defined in the U.S. Criminal Code, 18 U.S.C. § 2331) by a federal magistrate or judge "in any district in which activities related to the terrorism may have occurred," even if such locales are ordinarily outside the magistrate's or court's jurisdictional district); § 221, 115 Stat. at 292 (codified at 22 U.S.C.A. § 7205 (West Supp. 2003)) (imposing trade sanctions against the "Taliban or the territory of Afghanistan controlled by the Taliban," and all entities in Syria and North Korea); § 222, 115 Stat. at 292–93 (not codified, but published as 18 U.S.C.A. § 3124 note (2000 & West Supp. 2003)) (clarifying that providers of wire or electronic communication service are not required to assume any additional technical obligation, and that while such providers, landlords, and others must provide facilities or technical support in connection with law enforcement's execution of court orders or warrants authorizing the installation of pen registers or track and trace devices, they are to be reasonably compensated for doing so). These sections do not sunset, as provided in Section 224(a)–(b) of the USA PATRIOT Act, which expressly provides for all of the sections of Title II, *other than* these Sections, to sunset on December 31, 2005. § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note (2000 & West Supp. 2003)). Even those sections that do sunset will continue in effect after December, 2005, as they apply to then ongoing foreign intelligence investigations and to "any particular offense or potential offense that began or occurred before [December 31, 2005]." *Id.* § 224(b), 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note). The Justice Department has already proposed amendments of these and other provisions of the USA PATRIOT Act to continue and expand the law's controls.

12. Michael A. Olivas, *IIRIRA, The DREAM Act, and Undocumented College Student Residency*, 30 J.C. & U.L. 435 (2004); Cynthia J. Larose, *International Money Laundering Abatement and Anti-Terrorism Financing Act of* 2001, 30 J.C. & U.L. 417 (2004).

considered a delivery system for such materials.[13] Section 175(a) of the U.S. Criminal Code remains in effect and provides that anyone who "*knowingly* develops, produces, stockpiles, transfers, acquires, retains, or possesses *any* biological agent, toxin, or delivery system *for use as a weapon*," not including (under § 175(b)), activities that are prophylactic, protective, or peaceful, or who knowingly helps a foreign state or organization to do so, or who attempts to do these things, may be punished by criminal fines of up to $500,000 for entities and by imprisonment for any term of years or for life, criminal fines of up to $250,000, or by both, for individuals, both subject to increase or decrease for certain factors such as whether the individual or entity has profited financially or caused another to experience financial loss as a consequence of the criminal act.[14]

Section 817(1) of the USA PATRIOT Act amends § 175(b) of the U.S. Criminal Code, renumbering this section as 175(c) and redefining "[f]or use as a weapon" as this phrase is used throughout § 175 to include "development, production, transfer, acquisition, retention, or possession of any biological agent, toxin, or delivery system for other than prophylactic, protective, bona fide *research*, or other peaceful purposes."[15] This revision makes it clear that possession for a "bona fide research purpose" is not included in the definition of "for use in a weapon," as used in any subsection of § 175.

Section 817(1) then creates a new § 175(b), adding as an additional offense "*knowingly possess[ing]* any biological agent, toxin, or delivery system *of a type or in a quantity* that, under the circumstances, is *not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose.*"[16] This offense excludes any biological agent or toxin that is in its natural environment, meaning that the agent or toxin "has not been cultivated, collected, or otherwise extracted from its natural source."[17] This additional offense makes the mere knowing possession of agents or toxins a crime under certain circumstances, even if it is not known that the agents or toxins or their delivery systems are "for use as a weapon."[18] Such offense is punishable by up to ten years in prison, or criminal fines of up to $250,000, or both for individuals, and by criminal fines of up to $500,000 for entities, both subject to increase or decrease for certain factors such as whether the individual or entity has profited financially or caused another to lose financially as a consequence of the criminal act.[19]

New § 175(b) of the U.S. Criminal Code expands the criminal prohibition beyond knowing involvement with biological materials for use as a weapon. This section makes it a crime for the university or college, as well as for the individual

13. USA PATRIOT Act § 817(1), 115 Stat. at 385–86 (codified at 18 U.S.C.A. § 175 (2000 & West Supp. 2003)).

14. 18 U.S.C.A. § 175(a), (b) (2000 & West Supp. 2003); § 3571(b)–(d) (2000) (emphasis added).

15. USA PATRIOT Act § 817(1), 115 Stat. at 385 (codified at 18 U.S.C.A. § 175(c) (2000 & West Supp. 2003)) (emphasis added).

16. *Id*. § 817(1), 115 Stat. at 385 (codified at 18 U.S.C.A. § 175(b)) (emphasis added).

17. *Id.*

18. *Id*.

19. 18 U.S.C.A. §§ 175(b), 3571(b)–(d).

researcher or other personnel (such as research support staff, purchasing staff, or shipping and receiving staff), to possess any biological agent or toxin or related equipment of a type or in a quantity that is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose.[20] And outsiders such as federal law enforcement and ultimately the courts, not the researchers, will decide what is "reasonably justified," making it critical for institutions and individuals to view the law from a law enforcement perspective. The section criminalizes a wide range of activities and omissions involving biological agents and toxins and their delivery systems, and requires a significant reorientation for academic researchers who have not been accustomed to strict controls on how long excess materials are retained or on how much of a material is acquired in the first place. Regarding research from a law enforcement perspective is not a natural act in our academic culture.

Federal law enforcement officials take these provisions very seriously as an anti-bioterrorism measure, and academic researchers have found themselves to be the target of serious criminal investigations by the Federal Bureau of Investigation ("FBI") and to be subject to federal prosecution for retaining biological agents beyond the time when they are being actively used in research,[21] or for forgetting that an agent or toxin has been destroyed and accidentally reporting it missing,[22]

20. USA PATRIOT Act § 817(1), 115 Stat. at 385 (codified at 18 U.S.C.A. § 175(b)). Unlike the prohibition in Section 817(2) of the USA PATRIOT Act, which created 18 U.S.C. § 175b to prohibit certain individuals from possessing, receiving, or transporting biological agents and toxins listed and not exempted under the regulations implementing Section 511(d)(1) of the Antiterrorism and Effective Death Penalty Act of 1996 ("AEDPA") and its successor, Section 817(1) of the USA PATRIOT Act amends the U.S. Criminal Code to prohibit certain activities involving *any* biological agent or toxin, or related equipment, that are not "reasonably justified" for prophylactic, bona fide research or other peaceful purposes, without regard to whether the agent or toxin is listed in or exempted from regulations and without any specific quantity thresholds. *Id*.; *supra* notes 15, 16.

21. *See* Courtney Lowery, *Univ. of Connecticut Student Faces Federal Charge of Possession of Anthrax,* CHRON. OF HIGHER EDUC. (July 24, 2002), *available at* http://chronicle.com/prm/daily/2002/07/2002072401n.htm (a graduate student at the University of Connecticut was charged by federal prosecutors under the USA PATRIOT Act for allegedly failing to dispose of two vials of anthrax-infected tissue that was no longer needed for research when he was told to do so during a routine freezer cleaning during which the vials, left in the freezer since the late 1960s, were discovered; student is permitted to participate in a program of "community service, counseling and monitoring by the prosecutors and probation officers" in lieu of prosecution because he cooperated with the FBI and Justice Department in their investigation).

22. In January 2003, a researcher at Texas Tech University reported to federal law enforcement that approximately thirty vials of bubonic plague bacteria-infected samples were missing from his laboratory where he was studying the effectiveness of antibiotics on the plague. The researcher then remembered that he had destroyed the material. He was prosecuted in federal court. Although he was acquitted of charges relating to making false reports to federal law enforcement, the researcher endured a full trial and was convicted of other charges relating to research misconduct. *See* United States v. Butler, No. 5:03-M-10 (N.D. Tex. Apr. 10, 2003); Megan Rooney, *Vials of Bubonic Plague Are Reported Missing, Then Found, at Texas Tech U.*, CHRON. OF HIGHER EDUC. (Jan. 16, 2003), *available a*t http://www.chronicle.com/prm/daily/2003/01/2003011605n.htm and http://www.utexas.edu/opa/news/headlinenews/03news/0116.pdf. Katherine S. Mangan, *Texas Tech Professor, Accused of Mishandling Plague Samples, Is Convicted on Some Charges,* CHRON. OF HIGHER EDUC. (Dec. 2,

apparent mistakes that would not be remarkable in academic research settings. Academic researchers are being held accountable by federal law enforcement to a higher standard of biological materials management than is customary in academia. Such researchers must know the type and quantity of biological agents, toxins, and related equipment they have at all times, must have good controls to acquire only the quantities they need, and must destroy or dispose properly of such materials when they are no longer needed in research.

It is critical that the university or college inform all of its research groups that use, develop, produce, or possess *any* biological agents or toxins (or related equipment that may be considered to be a distribution system for such agents or toxins) regarding the substance of these federal criminal laws and the serious criminal liability that they as individuals, as well as the institution, may incur for violations. Part III.B of this article provides suggestions for a compliance program that is designed to minimize the burden on researchers and the likelihood of inadvertent violations of the USA PATRIOT Act and its companion federal act, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 ("BPARA").[23]

B. Select Biological Agents and Toxins

Section 817(2) of the USA PATRIOT Act adds § 175b to the U.S. Criminal Code, prohibiting any "restricted person" from shipping, transporting, possessing, or receiving biological agents or toxins listed and not exempted under the regulations implementing Section 511(d)(1) of the Antiterrorism and Effective Death Penalty Act of 1996 ("AEDPA"),[24] and making such activities by a restricted person a federal crime.[25] This prohibition applies to the individual, not to the institution and, in addition to covering individuals who are researchers using listed, non-exempt agents or toxins, may cover individuals who are responsible for arranging for, or undertaking shipping, receiving, transportation, storage, or other activities involving listed, non-exempt agents or toxins.[26] Violations by individuals of new Section 175b are subject to criminal penalties of up to ten years

2003), *available at* http://chronicle.com/weekly/v50/i16/16a01801.htm.

23. Pub. L. No. 107-188, 116 Stat. 594 (2002) (to be codified in scattered sections of 7, 18, 21, 29, 38, 42, 47 U.S.C.) [hereinafter BPARA]. *See* Centers for Disease Control and Prevention, Select Agent Program: FAQ for New Regulation, *available at* http://www.cdc.gov/od/sap/faq.htm (last visited Apr. 4, 2004) [hereinafter CDC FAQ].

24. Pub. L. No. 104-132, 110 Stat. 1214 (1996) (codified as amended in scattered sections 7, 8, 15, 18, 19, 21, 22, 28, 40, 42 U.S.C.) [hereinafter AEDPA]. The AEDPA's regulations at 42 C.F.R. § 72.6(h), (j) (referred to, *infra* note 31, in Appendix A) list select biological agents and toxins that are subject to registration requirements of the Secretary of Health and Human Services, Centers for Disease Control and Prevention, and exempts certain agents and toxins, including toxins with a Lethal Dose 50 "for vertebrates of more than 100 nanograms per kilogram of body weight [ ] used for legitimate medical purposes or biomedical research" or not being adequately potent to pose a severe risk to human health. 42 C.F.R. § 72.6(h) (2003); CDC FAQ, *supra* note 23.

25. USA PATRIOT Act § 817(2), 115 Stat. at 385–86 (codified at 18 U.S.C.A. § 175b (West Supp. 2003)).

26. *See id*., 115 Stat. at 386.

in prison and/or up to $250,000 in fines, subject to increase or decrease for certain mitigating or aggravating factors.[27] Although the prohibition applies directly to the individual, the institution could suffer adverse publicity and unwanted law enforcement attention if its researcher were to violate the prohibition. The enactment of BPARA, which is companion legislation to the USA PATRIOT Act, extends an obligation to the institution to not allow access to select agents and toxins to "restricted persons," as addressed in Part III of this article.

Individuals who are "restricted persons" under the USA PATRIOT Act are not permitted to continue to possess the relevant biological agents and toxins, or to ship, receive, or transport them, or, with the enactment of the BPARA, to have access to them.[28] Any support, custodial, and shipping and receiving staff who is a restricted person and who may need to undertake or arrange for any of the prohibited activities, must at least be reassigned to work that does not involve proscribed activities with listed, non-exempt agents or toxins and may lose his or her position if this is not possible;[29] and any researcher who is a restricted person must abandon research involving such agents or toxins and change the focus of his or her career, very significant effects indeed.

A "restricted person" under the USA PATRIOT Act is anyone who:

> [1] *is* under indictment for, or *has been* convicted of, a crime punishable by imprisonment for over one year (e.g., felonies, including certain moving motor vehicle violations), whether or not the person was actually punished with imprisonment]; or [2] *is* a fugitive from justice; or [3] *is* an unlawful user of any controlled substance [e.g, an illegal drug or a drug used illegally as defined and listed in 21 U.S.C. 802 and 812]; or [4] *is* an alien illegally or unlawfully in the United States; or [5] *has been* adjudicated as a mental defective or *has been* committed to any mental institution [which could arguably include anyone who has been self-committed for depression or drug or alcohol abuse, although this has not been decided by a court]; or [6] *is* an alien [including a legal alien in the United States, but not including a lawful permanent resident of the United States or green card holder who is a national of [Cuba, Iran, North Korea, Iraq, Libya, Sudan, or Syria] which includes individuals with dual citizenship of the United States and of any of the listed countries]; or [7] *has been* [dishonorably] discharged from the Armed Services of the United States.[30]

27. *See* 18 U.S.C.A. § 175b(c) (West Supp. 2003), § 3571(b), (d) (2000).

28. USA PATRIOT Act § 817(2), 115 Stat. at 385–86 (codified at 18 U.S.C.A. § 175b(a)). *See infra* Part III.A, notes 55–57 and accompanying text; Part III.A.4.b, notes 115–19 and accompanying text.

29. Note that a custodian who merely cleans a laboratory where such materials are used would arguably not be engaging in a proscribed activity if he or she does not have "access" to the materials, meaning that such a person is escorted at all times by a person who is authorized to have access or the materials are adequately secured to prevent access. It would be prudent to obtain approval of any security measure other than escorts from the administering agency. *See* CDC FAQ, *supra* note 23; *infra* Part III.A.5.

30. USA PATRIOT Act § 817(2), 115 Stat. at 386 (codified at 18 U.S.C.A. § 175b(d)(2))

One might question whether the nation is more secure when a talented researcher cannot pursue important research (e.g., on effective treatment of disease caused by exposure to a dangerous agent) because he or she was once convicted of a moving motor vehicle violation or was successfully treated for alcoholism at a

(emphasis added). There are no reported cases interpreting the USA PATRIOT Act's definition of a restricted person or challenging the constitutionality of the Act's criteria for defining a restricted person. One may question whether the USA PATRIOT Act's definition of restricted person would be upheld in the event of a constitutional challenge. With the possible exception of the sixth criterion (i.e., aliens from the enumerated countries), however, the definition of restricted person does not appear to include any classification that receives heightened judicial scrutiny. Consequently, it is likely in most constitutional challenges that the government would have to show only that it has a rational basis for determining the categories of restricted persons in relation to achieving the Act's legitimate national security purposes, and that such determinations, as implemented by the executive branch, are not arbitrary or capricious. *See* City of Cleburne v. Cleburne Living Center, 473 U.S. 432, 440 (1985) (noting that legislation is presumed to be valid and will be sustained if the classification drawn by the statute is rationally related to a legitimate state interest); 5 U.S.C.A. § 706(2)(A) (1996 & West Supp. 2003) (arbitrary and capricious standard for administrative agency action). Moreover, where national security is involved, Congress is given considerable discretion. *See* Hirabayashi v. United States, 320 U.S. 81, 93 (1943). This standard requiring a reasonable relationship of the law's requirements to legitimate government purposes is generally easy to meet. The standard may be somewhat more difficult to meet, however, in narrow circumstances such as where an individual is determined to be a restricted person only because he or she was discharged dishonorably from the military due only to sexual orientation. In that particular case, there may be good arguments that the law should be held to violate the First Amendment or the Fourteenth Amendment (substantive due process or equal protection), made applicable to the federal government through the Fifth Amendment; however, the law otherwise is likely to be upheld.

In contrast to review of the classification of individuals as restricted persons under most of the USA PATRIOT Act criteria to which the reasonable relationship standard applies, the classification of individuals as restricted persons based only on their nationality is likely subject to a stricter standard of judicial review, the strict scrutiny standard. As the Supreme Court held in *City of Cleburne*, "race, alienage, or national origin . . . are so seldom relevant to the achievement of any legitimate state interest that laws grounded in such considerations are deemed to reflect prejudice and antipathy. . . . [T]hese laws are subjected to strict scrutiny and will be sustained only if they are suitably tailored to serve a compelling state interest." *City of Cleburne*, 473 U.S. at 440. Despite this heightened standard of judicial review, it may be difficult to prevail in a constitutional challenge of even this criterion. The enumeration of a limited list of countries in the definition of a restricted person is tied to those countries that are suspected to be state sponsors of terrorism, and arguably may be closely related to the USA PATRIOT Act's goal of preventing or deterring bioterrorist acts. In the current environment, the objective tailoring of criterion may be narrow enough to survive a challenge. The question under strict scrutiny is whether all legal aliens of such countries must be excluded from research with select biological agents and toxins in order to achieve the compelling interest of preventing bioterrorism.

It is important for academic institutions to document how the government is administering and enforcing the law to ensure that the relevant agencies are not doing so in a discriminatory fashion (e.g., against individuals of only certain religions) or in a manner that otherwise abuses the agencies' discretion. It is also important for academic institutions to document the adverse effect of the law on important research if the academic community seeks to influence the development of more effective laws against bioterrorism that will safeguard our nation without undermining the research that makes the United States an international leader of education, innovation, and the world economy. While such information may be of limited value in a constitutional challenge to the USA PATRIOT Act's restricted persons criteria, it would support reasoned arguments to Congress for amendments to the law.

mental institution.

In any event, it is clearly a foreign concept in academic settings that an individual would have to abandon research based on citizenship or on most of the other criteria defining a restricted person. Yet, this is the reality that researchers, colleges, and universities must face.

Academic institutions have addressed Section 817(2) of the USA PATRIOT Act in different ways. Some have notified researchers and others who may do work involving select biological agents and toxins of the USA PATRIOT Act's prohibitions, their individual responsibility, and the consequences of violations, and have asked each person to self-assess whether he or she is a "restricted person." Some have also asked such researchers and others to certify to the institution (e.g., through the vice president for research, counsel's office, or environmental, health, and safety office) that the person has performed such self-assessment and understands the prohibitions. Others have required such certification to include a further statement that the individual is not a "restricted person." Appendix A to this article includes examples of such self-assessment questionnaires.[31] Self-assessments are a good practice for informing and sensitizing researchers and other personnel on the USA PATRIOT Act's prohibitions and on the individual criminal penalties for violation of these prohibitions.

Although the USA PATRIOT Act does not require it, some institutions may have attempted to perform background checks on individuals whose work may involve select biological agents or toxins to verify independently that they are not restricted persons.[32] It is unclear how an academic institution could adequately undertake a background check for this purpose.[33]

More importantly, BPARA imbues the U.S. Attorney General with responsibility for undertaking background checks (called "security risk assessments") of individuals who will have access to certain biological agents and toxins, including assessments of whether such individuals are "restricted persons" under the USA PATRIOT Act.[34] This should eliminate the perceived need that some institutions had to undertake their own background checks and is a sensible allocation of responsibility between the academic institution and the Justice Department. Certain limited criminal and other records may be available to the general public; however, much of the necessary information is unavailable to private entities (and even to some law enforcement authorities), requires access to

31. For Appendix A, USA PATRIOT Act Self-Assessment Questionnaire and USA PATRIOT Act Compliance Form for Select Agents, visit The Journal of College and University Law, Symposium Webpage, *at* http://www.nd.edu/~jcul/USA_PATRIOT_Act/Appendix_A.pdf (last visited Apr. 4, 2004).

32. The author participated in the Council on Government Relations ("COGR") Task Force on Bioterrorism which learned that some COGR colleges and universities may have taken this approach.

33. There are companies that offer background checking services, but these generally do not fully cover the USA PATRIOT Act landscape.

34. *See infra* Part III.A.4 (addressing the scope of "security risk assessments" under BPARA).

records of other countries that may not maintain complete information nor make much information publicly available, and, in many cases, requires the consent of the individual whose records are being reviewed (e.g., medical records and student records). Consents should be obtainable, but institutions are cautioned not to assume more responsibility than the USA PATRIOT Act and BPARA require or more than the institution is capable of fulfilling, as there are attendant liabilities and operational complexities. If an institution relies on the Attorney General's background checks under the BPARA rather than conducting its own, the institution can better maintain an appropriate, non-law enforcement, relationship with its faculty, students, and staff, while at the same time better defending against or avoiding liability for inaccurate background checks.

Regardless of an institution's approach to implementation, a great deal of thought is necessary as to what the institution must do, and what the institution is legally able to do, should a background check or self-assessment disclose that an individual is a restricted person. Clearly, an individual who is a restricted person is not permitted to possess, transport, ship, or receive listed and non-exempt biological agents and toxins (or as addressed below, to have unescorted access to them), even if the person's work or study requires these actions. What does the institution want to do if an individual cannot perform the requirements that are central to his or her position? Will the institution be legally permitted to reassign, discharge, or take other action respecting the individual? What laws governing privacy of information must be considered before disclosure of the results of a background check are made? If the institution's background check is inaccurate and an individual's career is harmed, or if the institution violates its own policies and procedures or contracts, or any laws and regulations governing privacy, labor, or employment, the institution's relationship with its constituents will be damaged and the institution may also be exposed to liability.

The institution should review and confer with counsel on the institution's employment and privacy policies and procedures, its employment and labor contracts, and the applicable state and federal employment, labor, and privacy law requirements, to ensure that the institution has a plan and process in place for responding to an adverse background check or security risk assessment appropriately for all concerned and without incurring liability. Federal and state laws governing privacy of medical and other individually identifiable information apply to obtaining much of the relevant information and to the disclosure of individually identifiable information to third parties; these laws often require the consent of the affected individual prior to disclosure.[35] Any consents must comply

35. *See, e.g.,* Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681u (2000); 10 C.F.R. § 15.23 (2004); 49 C.F.R. § 1018.21 (2003); 38 C.F.R. § 36.4337 (2003) (requiring prior notice to the subject of an investigative consumer report (including reports on an individual's credit, character, general reputation, personal characteristics, and mode of living such as credit history, employment history, education, legal proceedings, citizenship, medical, and other background information) by an outside reporting entity that an investigative consumer report will be undertaken, and if requested by the subject of the investigation, notice of the scope and purpose of the investigation; requiring the consumer's prior written authorization; requiring a copy of the report and a notice of the consumer's rights under the act to be provided to the subject of a report

with applicable laws, both in terms of the content and appropriateness of requiring the consent, and in terms of the institution's ability to disclose the information to the government and other third parties if it is determined that an individual is a restricted person. It is prudent for the legal and human resources offices of an academic institution to provide appropriate guidance to its academic and administrative offices that may be hiring individuals into positions affected by the USA PATRIOT Act and BPARA to assist them in making job offers, academic appointments, and status changes subject to the requirement that the individual be permitted under applicable laws to work with, possess, and have access to all materials that they may access in the course of their employment or work for the institution.

Before an institution can take these or any steps to address Section 817 of the USA PATRIOT Act, however, the institution must determine which research groups are using listed agents or toxins. Part III.B of this article provides guidance on how to make this determination as part of an institution's program to implement the USA PATRIOT Act and other anti-bioterrorism laws. Part III.B also provides sample consent language that addresses certain federal privacy law requirements, as well as sample language for employment or appointment offer letters.

The BPARA affects Section 817(2) of the USA PATRIOT Act in one additional respect that is worthy of note. The BPARA repeals Section 511(d) of the AEDPA.[36] Section 511(d) of the AEDPA was the federal law that was in effect when the USA PATRIOT Act was enacted and under which the Secretary of Health and Human Services ("HHS") had already promulgated a list of regulated select biological agents and toxins and exemptions. Section 817(2) of the USA PATRIOT Act refers to the list of select biological agents and toxins and exemptions in the regulations implementing Section 511(d) of the AEDPA. Consequently, with the passage of the BPARA repealing Section 511(d) of the AEDPA and calling for new regulatory lists of agents and toxins to be promulgated, it is unclear whether the reference in Section 817(2) of the USA PATRIOT Act to the AEDPA's regulatory list and exemptions should be deemed to be replaced by a reference to the BPARA's regulatory list and exemptions. The

if any adverse action will be taken in partial or full reliance on the report; and limiting the recipients and the transfer of the report); FERPA, 20 U.S.C.A. § 1232g (2000 & West Supp. 2003) (along with its regulations at 34 C.F.R. § 99.1 (2003), prohibiting the disclosure of individually identifiable information on a student that is maintained by any federally funded educational institution without the prior written consent of the student, with limited exceptions); The Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18, 26, 29, 42 U.S.C.) [hereinafter HIPAA]; Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000), as modified by 67 Fed. Reg. 14,776 (Mar. 27, 2002), 45 C.F.R. §§ 160, 164 (electronic transactions) (imposing records security, training and access/distribution limitation requirements on covered entities concerning individually identifiable health information, "protected health information," to protect the privacy of such information and regulating electronic health care transactions by covered entities to protect the privacy of the information). State statutes also regulate these matters.

36. BPARA § 203, 116 Stat. 594, 647 (not codified, but published as 42 U.S.C.A. § 262a note (2003)).

BPARA does not expressly so provide, but the alternative is for the list and exemptions under the AEDPA's regulations to survive for the purpose of applying the prohibitions respecting "restricted persons" under Section 817(2) of the USA PATRIOT Act.

It is most reasonable to conclude that the BPARA intends to substitute its regulatory lists and exemptions in Section 817(2) of the USA PATRIOT Act for those under the AEDPA.[37] The Department of Health and Human Services, Centers for Disease Control and Prevention's ("CDC") regulations under Section 511(d) of the AEDPA, including the regulatory list of agents and toxins at 42 C.F.R. § 72.6(j) and exemptions under 42 C.F.R. § 72.6(h) and Appendix B,[38] implementing Section 511(d)(1) of the AEDPA, are

> deemed [by Section 203 of the BPARA] to have been promulgated under section 351A of the Public Health Service Act, as added by Section 201 of [the BPARA, and the] regulations . . . that were in effect on the day before the date of the enactment of [the BPARA] remain in effect *until modified* by the Secretary [of Health and Human Services] in accordance with such Section 351A and with Section 202 of [the BPARA].[39]

These regulatory provisions under the AEDPA are adopted on an interim basis by the BPARA and are deemed to be modified by the new regulations under the BPARA once they are promulgated.[40] Section 204 of the BPARA repeals Section 511(d) of the AEDPA, presumably subject to its regulations' preservation during

37. *See infra* Part III. Note that the exemptions are quite different under the respective regulations implementing the AEDPA and the BPARA, and some of the listed agents and toxins are different as well. Appendix B to this article lists the agents and toxins that are regulated under the BPARA and notes where this Act's list differs from the agents and toxins regulated under the AEDPA. *See infra* note 38. Although the Animal and Plant Health Inspection Service ("APHIS") of the U.S. Department of Agriculture ("USDA") also regulates importing into the United States and transporting interstate certain organisms, vectors, and plant pests. Viruses, Serums, Toxins, and Analogous Products, 9 C.F.R. § 122.1 (2004) (prohibiting the interstate transportation or importation of organisms which "may introduce or disseminate any contagious or infectious disease of animals" and animals that have been "treated or inoculated with organisms" or are diseased, without a permit from APHIS); and Federal Plant Pest Regulations, 7 C.F.R. § 330.200 (2004) (prohibiting knowing interstate movement or importation of plant pests without a permit from APHIS). The definitions of covered organisms, vectors and plant pests are very broad and not based on lists. APHIS' lists of agents and toxins that pose a severe threat to animal and plant health or products under the BPARA is new. *See* APHIS, High Consequence Livestock Pathogens and Toxins, *available at* http://www.aphis.usda.gov/vs/ncie/pdf/agent_toxin_list.pdf (last visited Apr. 4, 2004). *See infra* Part III.A.3 for an outline of the exclusions and exemptions under the BPARA, and *supra* note 24 for a summary of the key exemptions under the AEDPA's regulations. *See also* http://www.cdc.gov/od/sap/42CFR72.htm (last visited Apr. 4, 2004) for the list of agents and toxins and exemptions under the regulations implementing Section 511 of the AEDPA.

38. For Appendix B, Bioterrorism Act Regulated Agents and Toxins, visit The Journal of College and University Law, Symposium Webpage, *at* http://www.nd.edu/~jcul/USA_PATRIOT_Act/Appendix_B.pdf (last visited Apr. 4, 2004).

39. BPARA § 203, 116 Stat. at 647 (not codified, but published as 42 U.S.C.A. § 262a note) (emphasis added).

40. *Id.*

the interim period before the Secretary promulgates new regulations under the BPARA.[41] In addition, the BPARA's requirement that the Attorney General perform background checks of individuals who will have access to agents and toxins that are listed and not exempted under the BPARA's regulations (or under the AEDPA's regulations until the BPARA's regulations are adopted), directs the Attorney General to determine whether such individuals are "restricted persons" under the USA PATRIOT Act.[42] These provisions evidence Congress' intention to tie the USA PATRIOT Act and the BPARA for purposes of fighting bioterrorism, and to treat the BPARA as modifying the AEDPA's regulations.[43] Whether the prohibition under Section 817(2) of the USA PATRIOT Act is clear enough for a criminal prosecution based on possession of an agent or toxin that is covered by the BPARA, but not by the AEDPA, or vice versa, is an open issue. In any event, although the BPARA does not explicitly amend and replace the reference in Section 817(2) of the USA PATRIOT Act to the AEDPA's regulatory list of agents and toxins and exemptions for purposes of applying Section 817(2)'s restricted persons prohibitions, the relevant provisions of the AEDPA and its regulations have been repealed and federal law enforcement is applying the BPARA's regulatory list of agents and toxins and exemptions instead to implement the restricted persons prohibitions.

III. THE PUBLIC HEALTH SECURITY AND BIOTERRORISM PREPAREDNESS AND RESPONSE ACT OF 2002[44] ("BPARA")

Another federal law, the BPARA, was enacted by Congress and signed into law by the President on June 12, 2002, to further protect against the use of certain particularly dangerous biological agents and toxins in bioterrorism. Title II, Subtitle A, Section 201(a) of BPARA ("Title II") adds a new Section 351A to the Public Health Service Act,[45] which is a companion federal law to Section 817 of the USA PATRIOT Act. The USA PATRIOT Act continues to apply to individuals who are "restricted persons." Title II, Subtitle A is implemented by the Secretary of Health and Human Services ("HHS") and its Centers for Disease Control and Prevention ("CDC"). Title II, Subtitle B, creates the Agricultural Bioterrorism Protection Act of 2002 and is implemented by the Secretary of Agriculture and USDA's Animal and Plant Health Inspection Service ("APHIS").

41. *Id.* §§ 203, 204, 116 Stat. at 647 (not codified, but published as 42 U.S.C.A. § 262a note).

42. *Id.* § 201(a), 116 Stat. at 639–40 (codified at 42 U.S.C.A. § 262a (2003)) (adding Section 351A(e)(3) to the Public Health Service Act); § 212(e)(3), 116 Stat. at 649–50 (codified at 42 U.S.C.A. § 262a); 42 C.F.R. § 73.8; 9 C.F.R. § 121.8; 7 C.F.R. § 331.7.

43. *See also* H.R. Conf. Rep. No. 107-3448, at 118–20 (2002) (Congress intends the BPARA to connect Section 817(2) of the USA PATRIOT Act to the security risk assessment process under the BPARA); *c.f.* H.R. Rep. No. 107-231, at 10-1 (2001) (addressing consideration of relationship between USA PATRIOT Act "restricted persons" criteria and BPARA regarding the need "not to unnecessarily impede . . . research into diseases caused by . . . agents. . . .").

44. BPARA's implementing regulations are at 42 C.F.R. pt. 73, 7 C.F.R. pt. 331, and 9 C.F.R. pt. 121.

45. BPARA § 201(a), 116 Stat. at 637–46 (codified at 42 U.S.C.A. § 262a).

Violations of the BPARA are punishable by criminal fines of up to $500,000 for entities and criminal fines of up to $250,000, imprisonment for up to five years, or both, for individuals, and civil penalties of up to $250,000 for individuals and $500,000 for entities.[46]

This sweeping law challenges the open and collaborative culture of academic research in fundamental ways. The law restricts the free access of researchers to other researchers' laboratories and storage areas by isolating and imposing strict controls on research using certain biological materials and, except with strict controls and oversight, by excluding individuals who are not cleared through Attorney General background checks (and approved for access by the Secretary of HHS or Agriculture) from areas where such materials are used or stored.[47] Such controls, although aimed at physical security, have the effect of severely limiting the free exchange of ideas that arise when researchers visit their colleagues' laboratories. The controls required by the regulations that have been promulgated under this law are expensive to implement because they prohibit shared laboratory and storage areas by researchers who work with select agents and toxins and researchers who do not, and they often require capital renovations to be made to isolate and secure areas or facilities where these materials are used or stored. Some researchers have opted to change the way they do science or abandon research entirely in order to avoid being subject to the BPARA and its regulations.[48]

Title II is broader in its application than Section 817(2) of the USA PATRIOT Act or Section 511(e)–(g) of the AEDPA, applying to any institution, as well as to any individual, who possesses, uses, or transfers certain select biological agents and toxins that have the potential to pose a severe risk to human, animal, or plant health, or animal or plant products.[49] Such institutions and individuals may allow

46. *Id*. § 201(a), 116 Stat. at 637 (codified at 42 U.S.C.A. § 262a(i)) (adding Section 351A(i) to the Public Health Service Act) (establishing civil monetary penalties); § 212(i), 116 Stat. at 655–56 (codified at 7 U.S.C.A. § 8401(i) (West Supp. 2003)) (establishing civil monetary penalties); § 231, 116 Stat. at 660 (codified at 18 U.S.C.A. § 175b (West Supp. 2003)) (establishing criminal penalties); 18 U.S.C.A. § 3571 (2000) (criminal fines and sentences). *See also* CDC FAQ, *supra* note 23; APHIS, Questions and Answers About the Agricultural Bioterrorism Protection Act of 2002 (Nov. 2003), *at* http://www.aphis.usda.gov/lpa/pubs/fsheet_faq_notice/faq_ahbioterroismact.html (on file with author).

47. *See* BPARA § 201(a), 116 Stat. at 639–42 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e) to the Public Health Service Act); § 212(e), 116 Stat. at 649–52 (codified at 7 U.S.C.A. § 8401(e) (West Supp. 2003)).

48. *See* Anne Marie Borrejo, *Regulatory Overkill? Universities fear that Congress is asking for too much in regulating work on dangerous substances*, CHRON. OF HIGHER EDUC. at A25 (Jan. 31, 2003).

49. *See* BPARA § 201(a), 116 Stat. at 637–46 (codified at 42 U.S.C.A. § 262a); § 212, 116 Stat. at 647–56 (codified at 7 U.S.C.A. § 8401 (West Supp. 2003)). The AEDPA and its regulations required the registration of listed non-exempt agents only prior to their transfer or receipt. AEDPA § 511(d)–(e), 110 Stat. 1214, 1284–85 (not codified, but published as 42 U.S.C.A. § 262 note (2003)). The USA PATRIOT Act only prohibits "restricted persons" from shipping, transporting, possessing and receiving listed, non-exempt agents and toxins. USA PATRIOT Act § 817(2), 115 Stat. at 385–86 (codified at 18 U.S.C.A. § 175b (West Supp. 2003)).

"access" to select agents and toxins only to individuals who have been approved for access by the applicable Secretary and cleared through background checks by the Attorney General, or who are escorted by those who are cleared in accordance with implementing regulations.[50] The CDC further clarifies that the regulations apply to any entity or individual who possesses, uses, transfers, or has access to such agents and toxins in the United States, or who receives such agents or toxins from outside the United States.[51] "Access" is a broad term that may apply not only to researchers and others who work directly with listed agents and toxins, but also to custodial and shipping and receiving staff who enter areas where listed agents or toxins are stored, used, shipped, or received.[52] Export control laws and regulations continue to govern the transfer abroad of biological agents and toxins governed by the BPARA (as well as additional chemicals, agents, and toxins), provision of information about such materials to foreign nationals or U.S. citizens abroad, and provision of certain information about such materials to foreign nationals in the United States.[53] U.S. Department of Transportation laws and regulations continue to apply to transportation of agents and toxins as hazardous materials.[54]

A. Listed Agents and Toxins and Security Through Registration and Background Checks

Generally, Title II of BPARA and its implementing regulations prohibit any entity or individual from possessing, using, transferring, receiving, or having

APHIS' list of regulated agents and toxins under Section 212 of the BPARA and its regulations is new, although APHIS had previously regulated and continues to regulate the importation and inter-state transportation of certain organisms, diseased or treated animals, and plant pests. *See* 9 C.F.R. pt. 122 (2004); 7 C.F.R. § 330.200 (2004). *See also supra* note 37.

50. BPARA § 201(a), 116 Stat. at 638–42 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(b)–(e) to the Public Health Service Act); § 212(b)–(e), 116 Stat. at 647–52 (codified at 7 U.S.C.A. § 8401 (West Supp. 2003)); 42 C.F.R. § 73.8(b); 9 C.F.R. § 121.11; 7 C.F.R. § 331.10.

51. 42 C.F.R. § 73.2(a). *Cf.* 9 C.F.R. § 121.2; 7 C.F.R. § 331.2 (APHIS' regulations are less specific than are CDC's, and track Title II, Subtitles A and B, § 201(a) (adding Section 351A(a)–(g), (j)), § 212(a)–(g), (j)). Both CDC's and APHIS' BPARA regulations govern overlap agents and toxins. 42 C.F.R. § 73.5; 9 C.F.R. § 121.3(b). The BPARA defines overlap agents and toxins as those that are listed by both Secretaries of HHS and USDA at 42 C.F.R. §§ 73.1, 73.5 and 9 C.F.R. §§ 121.1, 121.3(b), respectively. BPARA § 221(a)(2), 116 Stat. at 657 (codified at 7 U.S.C.A. § 8411 (West Supp. 2003). CDC's regulations do not govern, but the Department of Commerce's regulations do primarily govern the export of select agents and toxins. *See* 15 C.F.R. pts. 301–799, 774, Supp. I (2003) (listing 1C 350-353). The Department of State's regulations also govern such exports. 22 C.F.R. pts. 120–130, § 121.1 (2003) (listings under Category XIV). The Department of Transportation's regulations primarily govern transportation of agents and toxins that are hazardous materials. *See* 49 C.F.R. pts. 171–180 (2003).

52. *See* CDC FAQ, *supra* note 23.

53. *See supra* note 51.

54. *Id. See also infra* Part VI (addressing export controls). Regulation of exports abroad and deemed exports in the United States of biological materials, chemicals, and certain related information and equipment is an area of heightened interest to federal agencies in their homeland security efforts. *See, e.g.,* Department of Defense, Inspector General's Report of March 25, 2004, Export Controlled Technology at Contractor, University, and Federally Funded Research and Development Center Facilities, *available at* http://www.dodig.osd.mil/Audit/reports/FY04/04-061.pdf.

access to listed, non-exempt biological agents and toxins within the United States, except for a "lawful purpose"[55] and unless and until the entity, any individual who owns or controls the entity, certain individuals who are responsible for BPARA compliance at the entity, and all individuals who will possess, use, transfer, or have unescorted access to the agents or toxins are registered with the Secretary of HHS or Agriculture,[56] as appropriate, following their clearance through background checks, referred to as "security risk assessments," to be conducted by the Attorney General.[57] Approval of registration is conditioned on the development and implementation of security, safety, training, emergency preparedness and response, record-keeping, and other measures in accordance with the regulations implementing the Act.[58] The BPARA required the Secretaries of HHS and Agriculture (collectively "Secretaries") to adopt regulations by mid-December 2002 to implement the Act.[59] The Secretaries published their regulations on December 13, 2002, within a few days of the deadline. [60]

55. *See* BPARA § 201(a), 116 Stat. at 637–46 (codified at 42 U.S.C.A. § 262a); § 212, 116 Stat. at 647–56 (codified at 7 U.S.C.A. § 8401); 42 C.F.R. § 73.3 ("[a]n entity or individual may not possess or use in the United States, receive from outside the United States, or transfer within the United States, a select agent or toxins unless such activities are conducted for a lawful purpose and in accordance with [these regulations]").

56. *See* BPARA § 201(a), 116 Stat. at 638–39 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(d) to the Public Health Service Act); § 212(d), 116 Stat. at 648–49 (codified at 7 U.S.C.A. § 8401); 42 C.F.R. § 73.7; 9 C.F.R. § 121.6–121.9; 7 C.F.R. § 331.5–331.8 (registration requirements).

57. *See* BPARA § 201(a), 116 Stat. at 639–42 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e) to the Public Health Service Act); § 212(e), 116 Stat. at 649–52 (codified at 7 U.S.C.A. § 8401); 42 C.F.R. § 73.8 ("[a]n entity may not possess or use in the United States, receive from outside the United States, or transfer within the United States, any select agent or toxin unless approved by the HHS Secretary or the USDA Secretary based on a security risk assessment by the Attorney General"); 9 C.F.R. §§ 121.8, 121.11; 7 C.F.R. §§ 331.7, 331.10.

58. 42 C.F.R. § 73.7(b)(2); 9 C.F.R. §§ 121.6, 121.7(b)–(c), 121.8; 7 C.F.R. §§ 331.5, 331.6(b), 331.7.

59. BPARA § 202(b), 116 Stat. at 646 (not codified, but published as 42 U.S.C.A. § 262a note (2003)); § 213(c), 116 Stat. at 657 (not codified, but published as 7 U.S.C.A. § 8401 note (West Supp. 2003)). Within 180 days after enactment of the BPARA, the HHS Secretary was required to promulgate an interim final rule for carrying out the provisions of § 351A of the Public Health Service Act (i.e., Title II of the BPARA), provided that the effective dates for such regulations must "minimize disruption of research or educational projects that involve [listed] biological agents and toxins . . . and that were underway as of the effective date of such rule." *Id.* § 202(b)–(c), 116 Stat. at 646–47 (not codified, but published as 42 U.S.C.A. § 262a note).

60. The CDC and APHIS published regulations on December 13, 2002, with phased-in effective dates for different provisions to minimize the effect on ongoing research and education. 42 C.F.R. § 73.0; 9 C.F.R. § 121.0; 7 C.F.R. § 331.0. This article will not address the complicated phase-in provisions because the entire regulation became effective on November 12, 2003. 42 C.F.R. § 73.0; 9 C.F.R. § 121.0; 7 C.F.R. § 331.0. The CDC's regulations at 42 C.F.R. pt. 73 under the BPARA supercede the CDC's regulations at 42 C.F.R. pt. 72.6 governing select biological agents and toxins under the AEDPA. 42 C.F.R. § 73.0. The CDC's regulations under the AEDPA and the relevant provisions of Section 511 of the AEDPA establishing a list of agents and toxins that were subject to registration prior to transfer or shipping, and exemptions, were repealed by the BPARA. BPARA §§ 203, 204, 116 Stat. at 647 (not codified, but published as 42 U.S.C.A. § 262 note). *See supra* notes 36–43 and accompanying text.

USDA had never been required by law to publish a list of biological agents and toxins

1. Coordination of Two Sets of Regulations: Health and Human Services and Agriculture

Although the BPARA contemplates two sets of regulations, the Secretaries must coordinate their regulations and the procedures governing those select agents and toxins that are regulated by both HHS and USDA (referred to as "overlap agents and toxins").[61] Coordination is intended to minimize conflicts in the two Secretaries' regulations, as well as to ease any administrative burden on the regulated community.[62] In a memorandum of understanding, the Secretaries must provide for a single registration system for overlap agents and toxins (including provisions for a single form and filing process for registration and for background checking, sharing of registration information, joint record-keeping, and enforcement by either Secretary on behalf of both).[63] Ultimately, the Secretaries are to issue joint regulations governing overlap agents and toxins.[64] Coordination

to be regulated in a similar approach and scope to that of HHS' regulation of select biological agents and toxins under the AEDPA. *See supra* notes 37, 49. USDA regulates interstate transportation and importation of plant pests and diseased or treated animals and organisms, but defines them broadly rather than listing them. *See id*.; 9 C.F.R. § 122.1 (2004); 7 C.F.R. §§ 330.100, 330.200 (2004). Consequently, the BPARA did not have to repeal another law or provide for the continued effectiveness of regulations under any other law for an interim period. Section 213(a) of the BPARA requires the Secretary of Agriculture, within sixty days after enactment of the BPARA, to promulgate an interim final rule that establishes an initial list of biological agents and toxins that the Secretary has determined under BPARA § 212(a)(1) "has the potential to pose a severe threat to animal or plant health or animal or plant products." BPARA § 212(a)(1)(A), 116 Stat. at 647 (codified at 7 U.S.C.A. § 8401). Section 213(c) of the BPARA requires the Secretary of Agriculture to promulgate an interim final rule that implements the remainder of Section 212 of the BPARA within 180 days after its enactment. *Id*. § 213(c), 116 Stat. at 657 (not codified, but published as 7 U.S.C.A. § 8401 note). Just as Section 203 addresses the effective date for the Secretary of HHS' regulations, Section 213(d) of the BPARA requires the Secretary of Agriculture's regulations to have effective dates that "minimize disruption of research or educational projects that involve [listed] biological agents and toxins . . . that were underway as of the effective date of such rule." *Id*. § 213(d), 116 Stat. at 657–58 (not codified, but published as 7 U.S.C.A. § 8401 note).

The Secretary of Agriculture's Animal and Plant Health Inspection Service ("APHIS") published two sets of regulations on December 13, 2002, one relating to agents and toxins that "have the potential to pose a severe threat to both human and animal health, to animal health or to . . . animal products." 9 C.F.R. § 121.2. The second regulation relates to agents and toxins that "have been determined to have the potential to pose a severe threat to plant health or . . . plant products." 7 C.F.R. § 331.2.

61. An "overlap agent or toxin" is defined as one "that is listed [by the Secretary of HHS] pursuant to section 315A(a)(1) [sic] of the Public Health Service Act, as added by section 201 of [the BPARA] and . . . [by the Secretary of Agriculture] pursuant to section 212(a)(1) of [the BPARA]." BPARA § 221(a)(2)(A), 116 Stat. at 657 (codified at 7 U.S.C.A. § 8411 (West Supp. 2003)).

62. *Id.* § 221(b), 116 Stat. at 657 (codified at 7 U.S.C.A. § 8411).

63. *Id.* § 221(c), 116 Stat. at 658 (codified at 7 U.S.C.A. § 8411). The Secretaries may have entered into a memorandum of understanding, but it has not been published**.** At the time this article went to the printer, a Freedom of Information Act, 5 U.S.C. § 552, request to HHS and USDA for this memorandum of understanding was acknowledged without any substantive response and was still pending.

64. *Id*. § 221(d), 116 Stat. at 659 (codified at 7 U.S.C.A. § 8411).

also supports "appropriate availability of biological agents and toxins for legitimate biomedical, agricultural or veterinary research, education or other such purposes" and the inclusion of registration information from both Secretaries in a national database.[65] The availability of select agents and toxins for research and education is an important requirement of the BPARA that must be balanced with the Act's requirements for security.[66]

2. Listed Agents and Toxins

Central to the BPARA's implementation is its requirement that the Secretaries of HHS and Agriculture must create regulatory lists of covered select biological agents and toxins. The Secretary of HHS must create a list of biological agents and toxins that have been determined by the Secretary "to pose a severe threat to public health and safety" for regulation under the BPARA;[67] and this list is to

65. *Id*. § 221(b)(3)–(4), 116 Stat. at 658 (codified at 7 U.S.C.A. § 8411). CDC and APHIS each promulgated its own regulations and there are many differences in form and some differences in substance. *See* 42 C.F.R. pt. 73.0 (2003); 9 C.F.R. pt. 121.0 (2004); *see also, e.g., infra* Parts III.A.5, 8–11. The CDC's regulations tend to be more detailed and prescriptive. In harmonizing the two sets of regulations, particularly for overlap agents and toxins, the stricter and more specific requirements of each set is likely to govern.

Site-specific, transfer-specific, and registered person-specific information in the federal database or otherwise held by HHS, USDA, the Justice Department, the Department of Transportation, or other agencies to which information may have been provided, is exempt from disclosure under the Federal Freedom of Information Act, 5 U.S.C. § 552. BPARA § 201(a), 116 Stat. at 643–45 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(h) to the Public Health Service Act); § 212(h), 116 Stat. at 654–55 (codified at 7 U.S.C.A. § 8401 (West Supp. 2003)) (providing that federal agencies shall not disclose under 5 U.S.C. § 552 information from the federal database to the extent that it is site, registered-person or transfer specific, or that it relates to information on a theft or release of listed, non-exempt agents or toxins, or that it relates to an inspection or evaluation that is person and agent or toxin identity or location specific if the agency determines that disclosure "would endanger public health or safety" or "would endanger animal or plant health").

66. *See* BPARA § 201(a), 116 Stat. at 638 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(b)(4) to the Public Health Service Act); § 212(b)(4), 116 Stat. at 648 (codified at 7 U.S.C.A. 8401); 148 Cong. Rec. S4773–75 (daily ed. May 23, 2002) (statement of Sen. Kennedy), 148 Cong. Rec. S4776–77 (daily ed. May 23, 2002) (statement of Sen. Gregg) (demonstrating that Congress was concerned about ensuring the availability of biological agents and toxins for research and education and wanted this need to be balanced with need to protect against their misuse).

67. BPARA § 201(a), 116 Stat. at 637 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(a)(1)(A) to the Public Health Service Act). Section 201 requires the Secretary of HHS to undertake a biennial or more frequent review in order to revise the list as necessary. *Id.*, 116 Stat. at 638 (adding Section 351A(a)(2) to the Public Health Service Act). In considering whether to list an agent or toxin, the Secretary is to consider (a) the "effect on human health of exposure to the agent or toxin," (b) "the degree of contagiousness" and the method of transmission to humans of the agent or toxin, (c) "availability and effectiveness" of drugs, immunization and treatments to "treat and prevent any illness resulting from infection by the agent or toxin," and (d) "any other criteria . . . that the Secretary considers appropriate." *Id*., 116 Stat. at 637–38 (adding Section 351A(a)(1)(B)(i) to the Public Health Service Act). The Secretary is to consult with "appropriate Federal departments and agencies and with scientific experts representing appropriate professional groups" in developing the list. *Id.*, 116 Stat. at 638 (adding Section

supercede and formally expand the pre-existing list of select agents and toxins that were included in the CDC's regulations under the AEDPA.[68] The Secretary of Agriculture must create lists of biological agents and toxins that have "the potential to pose a severe threat to animal or plant health, or to animal or plant products" for regulation under the BPARA.[69] The Secretaries are to review and update their respective lists at least biennially.[70] Appendix B[71] of this article contains the regulatory lists of agents and toxins that were promulgated by the CDC and by the APHIS to implement these requirements of the Act.[72]

In addition to regulating the named agents and toxins, the BPARA and its regulations also govern HHS and overlap agents and toxins that fall under any of the following categories of genetic elements, recombinant nucleic acids, and recombinant organisms:

> (a) select agent viral nucleic acids (synthetic or naturally derived, contiguous or fragmented, in host chromosomes or in expression vectors) that can encode infectious and/or replication competent forms of any listed select agent virus; [(b)] nucleic acids (synthetic or naturally derived) that encode for functional forms of any [listed] toxin if the nucleic acids are in a vector or host chromosome, can be expressed in vivo or in vitro, or are in a vector or host chromosome and can be expressed in vivo or in vitro; and [(c)] [listed] viruses, bacteria,

351A(a)(1)(B)(ii) to the Public Health Service Act).

68. *Id.* § 201(a), 116 Stat. at 638, 639–40 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(b)–(e) to the Public Health Service Act). Note that subsection (e) requires security "commensurate with the risk such agent or toxin poses to public health," permitting different levels of security requirements based on the risks of particular agents or toxins. *Id.* § 201(a), 116 Stat. at 639 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e) to the Public Health Service Act). Under this subsection, the Secretary is to consult with the Attorney General on the establishment of security requirements as part of the registration system. *Id.*

69. *Id.* § 212(a)(1)(A), 116 Stat. at 647 (codified at 7 U.S.C.A. § 8401 (West Supp. 2003)).

70. *Id.* § 201(a), 116 Stat. at 638 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(a)(2) to the Public Health Service Act); § 212(a)(2), 116 Stat. at 648 (codified at 7 U.S.C.A. § 8401). The next review should be in December, 2004, as the first and current lists were promulgated in December 2002.

71. *See* Appendix B, *supra* note 38.

72. *See* 42 C.F.R. § 73.4 (listing HHS select agents and toxins), § 73.5 (listing HHS select overlap agents) (2003); 9 C.F.R. § 121.3 (2004) (listing the USDA's human and animal-threatening agents and toxins and USDA overlap agents and toxins); 7 C.F.R. § 331.3 (2004) (listing the plant and plant product-threatening agents). The overlap agents are identical under the two regulations. Interesting issues arise concerning what is a listed, non-exempt agent or toxin. Is an animal that is inoculated with such an agent or toxin to be treated as a regulated agent or toxin itself, and, consequently, to be subject to the security and other requirements of the regulations that govern the regulated agent or toxin? The CDC has informally advised that the answer is yes if a recoverable or infectious agent or toxin is injected into an animal. E-mail from Kevin Beggs, Bio-Containment Laboratory Certification Specialist, Constella Health Sciences, CDC Contractor to, to Claudia Molina of Arnold & Porter (Feb. 2, 2004) (on file with author). If an animal ingests the agent or toxin in its natural environment, however, the animal is not governed by the BPARA regulations. *Id. See also supra* notes 37, 49, 60 (concerning APHIS' additional regulation of infected animal importation and interstate transport under 9 C.F.R. pt. 122).

fungi and toxins . . . that have been genetically modified.[73]

3. Exclusions and Exemptions from Regulation

Before complying with the detailed registration, security risk assessment (i.e., background check), security, training, record-keeping, and other requirements of the BPARA and its regulations, it is critical to determine whether an agent, toxin, or activity using an agent or toxin is excluded or exempted. The regulations exclude certain agents and toxins that would otherwise be regulated, and exempt others as specified in the BPARA.[74] The scientific and technical expertise of biosafety professionals and researchers is necessary to apply many of the exclusions and exemptions to particular facts. Appendix C[75] to this article includes a quick reference table to the available exclusions and exemptions.

An agent or toxin that is in its "naturally occurring environment" and has not been "intentionally introduced, cultivated, collected, or otherwise extracted from its natural source" is excluded from both the HHS and USDA regulations.[76] Also excluded from both agencies' regulations (except as noted) are: (a) "non-viable select agent organisms," "non-viable agents," and "nonfunctional toxins" (although

73. 42 C.F.R. § 73.4(e); 9 C.F.R. § 121.3(c).

74. *See* BPARA § 201(a), 116 Stat. at 642–43 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(g) to the Public Health Service Act); § 212(g), 116 Stat. at 652–54 (codified at 7 U.S.C.A. § 8401) (emphasis added). Under these provisions:

> 1. The Secretary *must* exempt from the regulations:
>
> *"clinical or diagnostic laboratories* and other persons who *possess, use or transfer* [specimens] for diagnosis, verification or proficiency testing", provided that the agents and toxins are reported to the Secretary and, if required by federal, state or local law, to other authorities, and that the agents and toxins are *transferred or destroyed* in accordance with the Secretary's regulations; and
>
> *"products* that *are, bear or contain*" listed agents/toxins and are *"cleared, approved, licensed or registered* under . . . The Federal Food, Drug and Cosmetic Act, Section 351 of the Public Health Service Act/[Antiterrorism and Effective Death Penalty Act,] . . . the Virus-Serum-Toxin Act, [or] the Federal Insecticide, Fungicide and Rodenticide Act,". . . [u]nless the Secretary determines by order that additional regulation of a specific product is required to protect public health and safety.
>
> 2. The Secretary *may* exempt from the regulations:
>
> *"Investigational product[s]* that *[are], bear, or contain"* listed [agents/toxins] being used in an investigation authorized under any Federal Act if the "Secretary determines that . . . additional regulation . . . is not necessary to protect [public health and safety.]" [This exemption is subject to an application process to be specified in regulations.]
>
> 3. The Secretary *may temporarily* exempt a person [from the regulations for 30 days, plus one 30-day extension,] if the Secretary determines [the] exemption is necessary [for] timely participation of the person in a response to a domestic or foreign [public health] emergency [or certain agricultural emergencies] that involve [a listed agent or toxin.]"

Id.

75. For Appendix C, Quick Reference Table: Bioterrorism Act Regulatory Exclusions and Exemptions, visit The Journal of College and University Law, Symposium Webpage, *at* http://www.nd.edu/~jcul/USA_PATRIOT_Act/Appendix_C.pdf (last visited Apr. 4, 2004).

76. 42 C.F.R. §§ 73.4(f)(1), 73.5(f)(1); 9 C.F.R. § 121.3(e) (2004); 7 C.F.R. § 331.3(b) (2004).

APHIS' regulations at 9 C.F.R. § 122 continue to govern interstate transfer and importation of genetic elements or subunits of these animal agents and toxins),[77] (b) vaccine strain of Junin virus (Candid #1), of Rift Valley fever virus (MP-12), and of Venezuelan Equine encephalitis virus (TC-83) (all of which are exempt from HHS regulation), "genetic elements or subunits of listed agents or toxins [if they] are not capable of causing disease" (which are excluded from USDA regulation, although the interstate transport and importation of such animal agents and toxins continue to be subject to APHIS' regulations at 9 C.F.R. § 122), and genetic elements that are not capable of "encod[ing] infectious and/or replication competent forms" of listed viruses (which are excluded from the definition of regulated genetic elements of HHS agents),[78] and (c) per Principal Investigator volumes of certain listed HHS and overlap toxins as noted in Appendix C[79] to this article.[80] Upon application by an entity, the CDC on behalf of the HHS Secretary or the APHIS Administrator on behalf of the Agriculture Secretary, as applicable, may exclude "attenuated strains" of agents and toxins or overlap agents and toxins, in the case of HHS agents "upon a determination [by CDC that HHS agents or toxins] do not pose a severe threat [to the] public health and safety" and, in the case of overlap agents or toxins, upon a determination (by CDC or APHIS) that the overlap agents or toxins do not pose such threat to public health and safety and also "do not meet the criteria [of 9 C.F.R. § 121] for inclusion," and in the case of animal agents upon a determination (by APHIS) that the agents do not "pose a severe threat to both human and animal health, to animal health, or to animal products."[81]

An entity is exempt from the CDC regulations relating to HHS agents and toxins as well as HHS/APHIS overlap agents and toxins, and from the APHIS regulations relating to animal and plant agents and toxins, if the entity's only activities with such listed agents and toxins involve specimens or isolates from specimens for diagnosis, verification, or in the case of HHS agents and toxins, overlap agents and toxins, and APHIS animal agents and toxins, proficiency testing. The CDC regulations at 42 C.F.R. § 73.14 relating to transfers in the

77. 42 C.F.R. §§ 73.4(f)(2), 73.5(f)(2); 9 C.F.R. § 121.3(f)(1) & n.1, 121.3(f)(2); 7 C.F.R. § 331.3(c)(1).

78. 42 C.F.R. §§ 73.4(f)(3), 73.5(f)(3), 73.4(e)(1), 73.5(e)(1); 9 C.F.R. § 121.3(f)(2) & n.2; 7 C.F.R. § 331.3(c)(2).

79. *See* Appendix C, *supra* note 75.

80. 42 C.F.R. §§ 73.4(f)(4), 73.5(f)(4); 9 C.F.R. § 121.3(f)(3).

81. 42 C.F.R. § 73.4(f)(5) (attenuated strains of HHS agents and toxins), § 73.5(f)(5) (attenuated strains of overlap agents); 9 C.F.R. § 121.3(g) (USDA's attenuated strains of animal agents and toxins and overlap agents). Applications may be made to either the Secretary of HHS (through the Administrator of the CDC) or the Secretary of Agriculture (through the Administrator of APHIS) to request an exclusion for an attenuated strain of an overlap agent or toxin. CDC and APHIS will confer with one another before making a determination and will issue a written determination, which will also be published in the Federal Register. *See* CDC, Select Agent Program, *at* http://www.cdc.gov/od/sap/exclusion.htm (last visited Apr. 4, 2004). The exclusion is effective upon issuance of the written determination. 42 C.F.R. § 73.5(f)(5); 9 C.F.R. § 121.3(g). The APHIS regulations provide for reconsideration of an adverse determination by the APHIS Administrator, but a similar provision is not included in CDC's regulations. 42 C.F.R. § 73.5(f)(5); 9 C.F.R. § 121.3(g).

United States or from outside to inside the United States continue to apply, as do APHIS' regulations at 7 C.F.R. § 330 on the interstate transfer or importation of plant agents. There are also a number of conditions that must be met under each of the regulations to qualify for this exemption.[82]

HHS, USDA animal, and HHS/USDA overlap agents and toxins in products that "are, bear or contain listed select agents or toxins that are cleared, approved, licensed, or registered" under certain federal laws, namely the federal Food, Drug, and Cosmetic Act,[83] Section 351 of the Public Health Service Act,[84] Virus-Serum-Toxin Act,[85] or the federal Insecticide, Fungicide, and Rodenticide Act[86] are exempt from the BPARA and its regulations to the extent their use is "only for the approved purpose" and is in compliance with the applicable specified federal law.[87] This exemption will not be available or may be limited in its application, however, if the Secretary of HHS or Agriculture determines that it is necessary to make such materials subject to certain provisions of the BPARA's regulations in order to protect the public health (in the case of HHS) or animal or plant health or products (in the case of USDA).[88] In such event, the HHS Secretary or the APHIS

82. 42 C.F.R. § 73.6(a); 9 C.F.R. §§ 121.4(a)–(b), 121.5(a)–(b); 7 C.F.R. § 331.4(a) & n.1. BPARA § 201(a), 116 Stat. at 642 (codified at 42 U.S.C.A. § 262a (2000 & West Supp. 2003)) (adding Section 351A(g)(1) to the Public Health Service Act); § 212(g)(1)(B), 116 Stat. at 652–53 (codified at 7 U.S.C.A. § 8401 (West Supp. 2003)). APHIS does not list proficiency testing in the list of exempt activities for plant agents, but does exempt proficiency testing for overlap and animal agents and toxins. *See* 9 C.F.R. §§ 121.4, 121.5. To qualify for the exemption on the basis of diagnosis or verification testing, the entity must "immediately report" to the HHS Secretary through CDC the agents (if they are Variola major virus (Smallpox virus), Variola minor (Alastrim), Bacillus anthracis, Yersinia pestis, Botulinum neurotoxins, Francisella tularensis, Ebola viruses, Marburg virus, Lassa fever virus, or South American Haemorrhagic Fever virus (Junin, Machupo, Sabia, Flexal, Guanarito) or to the USDA Secretary through APHIS (for any listed agent or virus), as applicable, as well as to other authorities as may be required by federal, state, or local law. *See* 42 C.F.R. § 73.6(a)(2), (3); 9 C.F.R. §§ 121.4(a)(1), 121.5(a)(1); 7 C.F.R. § 331.4(a). Within seven days after identification, the entity must transfer the specimens or isolates to a facility qualified to receive them or must appropriately destroy the specimens or isolates (i.e., by autoclaving, incineration, sterilization or neutralization sufficient to render them inactive), record the identification and transfer or destruction of the specimens or isolates, and submit a notice on the appropriate CDC or APHIS form. *See* 42 C.F.R. § 73.6(a)(4), (5), (7); 9 C.F.R. §§ 121.4(a)(2), 121.5(a)(2); 7 C.F.R. § 331.4(a)(2). The entity must maintain the record for three years. *Id.* An entity must provide similar notices, transfer or destroy select overlap agents and toxins and APHIS animal agents and toxins, and keep records of such agents and toxins used for proficiency testing, but must transfer or destroy them and notify CDC or APHIS within ninety days after receipt for proficiency testing. *See* 42 C.F.R. § 73.6(a)(6), 9 C.F.R. §§ 121.4(b), 121.5(b).

83. 21 U.S.C. § 301 et seq. (2000).

84. 42 U.S.C. § 262 (2000).

85. 21 U.S.C. § 151 et seq. (2000).

86. 7 U.S.C. § 136 (2000).

87. 42 C.F.R. § 73.6(b); 9 C.F.R. §§ 121.4(c), 121.5(d). *See* BPARA §201(a), 116 Stat. at 642–43 (codified at 42 U.S.C.A. § 262(a)) (adding Section 351A(g)(2) to the Public Health Service Act); § 212(g)(1)(C)(i), (ii), 116 Stat. at 653 (codified at 7 U.S.C.A. § 8401 (West Supp. 2003)).

88. 42 C.F.R. § 73.6(b); 9 C.F.R. §§ 121.4(c), 121.5(d).

Administrator must issue an order to this effect.[89] APHIS also exempts "diagnostic reagents and vaccines that are, bear, or contain listed [animal] agents or toxins, also known as high consequence livestock pathogens or toxins, that are produced at USDA diagnostic facilities."[90]

Experimental or investigational products that "are, bear or contain" listed HHS, USDA animal, and HHS/USDA overlap agents or toxins and are being used in an investigation authorized by federal law are exempt if the Secretary of Agriculture (through the APHIS Administrator) or the Secretary of HHS (through the CDC) determines that regulation under the BPARA is not necessary to protect animal or plant health or products (APHIS) or public health (CDC). CDC allows for this exemption only if the specified federal laws are involved. The applicant for this exemption must submit a request on the appropriate APHIS or CDC form.[91]

There are also provisions under CDC's and APHIS' regulations for temporary, thirty day exemptions from regulation of HHS agents and toxins and HHS/USDA overlap agents and toxins, extendable for another thirty days, for domestic or foreign public health or agricultural emergencies.[92] Under the APHIS regulations there are temporary, up to three-year exemptions from regulation of animal and plant agents and toxins "on a showing of good cause" when consistent with protecting animal or plant health and products.[93]

4. Registration and Security Risk Assessment

If an exclusion or exemption does not apply, before an entity or any individual possesses, uses, receives, transfers, or has unescorted access to listed agents or toxins, the entity must register with one or both Secretaries, as applicable.[94] As a prerequisite to registration, the entity must receive all required clearances for the entity and all individuals who will possess or use listed agents or toxins, who are responsible for administering compliance with and implementation of the regulations, who will have unescorted access to listed agents or toxins, or, with limitations for certain academic institutions, who own or control the entity, from

89. 42 C.F.R. § 73.6(b); 9 C.F.R. §§ 121.4(c), 121.5(d). The CDC's regulations specify that such an order must be issued to the relevant entity; APHIS' regulations are silent on the addressee of the order. 42 C.F.R. § 73.6(b); 9 C.F.R. §§ 121.4(c), 121.5(d).

90. 9 C.F.R. § 121.5(c).

91. BPARA § 201(a), 116 Stat. at 642–43 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(g)(2)(C) to the Public Health Service Act); § 212(g)(1)(C)(iii), 116 Stat. at 653 (codified at 7 U.S.C.A. § 8401); 9 C.F.R. § 121.4(d) (exemption for overlap agents/toxins); 9 C.F.R. § 121.5(e) (exemption for experimental products with animal agents or toxins); 42 C.F.R. § 73.6(c) (exemption for experimental products with HHS agents and toxins and overlap agents/toxins). CDC form 0.1317 and APHIS form 2042 are available at http://www.cdc.gov/od/sap/forms/exempts.pdf (last visited Apr. 4, 2004) [hereinafter CDC Form and APHIS Form].

92. 42 C.F.R. § 73.6(d)–(e); 9 C.F.R. § 121.4(e)–(f).

93. 9 C.F.R. § 121.5(f) (exemption consistent with protecting animal health or products on a "showing of good cause" for up to three years); 7 C.F.R. § 331.4(b) (2004) (exemption consistent with protecting animal or plant health and animal or plant products on a "showing of good cause" for up to three years).

94. 42 C.F.R. § 73.7; 9 C.F.R. §§ 121.6–121.7; 7 C.F.R. §§ 331.5–331.6.

the U.S Attorney General through a "security risk assessment" process specified in the regulations.[95] The entity and individual must comply with the other requirements of the regulations, including those that require the entity to designate a "Responsible Official" with broad responsibilities for complying with and implementing the regulations, in order to satisfy the conditions to registration.[96] The Act authorizes the Secretaries to inspect persons (entities and individuals) who are subject to the regulations to ensure their compliance.[97] These inspections may occur as part of the registration process, and/or later to ensure that registered entities and individuals maintain compliance.[98]

The Responsible Official and any Alternate Responsible Official must have adequate expertise in biosafety and sufficient authority on behalf of the entity to administer implementation and compliance with the BPARA and its regulations. Because the Responsible Official and any Alternate Responsible Official must have authority over work of an entity's employees and must act on behalf of the entity, he or she should typically be an employee.[99] In any event, he or she must have authority to act on behalf of the entity concerning biological agents and toxins.[100]

The BPARA establishes the obligations that are applicable to registered persons (entities and individuals), to the Secretaries, and to the Attorney General, and the regulations generally reflect this allocation of responsibilities. It is important for an institution not to assume responsibilities that are allocated to the Secretaries or Attorney General because the institution's actions will not satisfy the Act's or regulations' requirements and the institution will be unnecessarily assuming exposure to liability, for example, if the institution makes a mistake in background checking.

Registered entities and individuals are required (a) to provide access to listed agents and toxins only to individuals who have a "legitimate need to handle or use" them;[101] (b) to submit "names and other identifying information" about such an

95. 42 C.F.R. §§ 73.3, 73.7–73.8 (requiring registration and clearance through security risk assessment in order for an entity or individual to possess, use or transfer listed select agents or toxins); 9 C.F.R. §§ 121.7, 121.8, 121.11; 7 C.F.R. §§ 331.6, 331.7, 331.10.

96. *See* 42 C.F.R. § 73.9. *See also* 9 C.F.R. § 121.2(b)–(c); 7 C.F.R. § 331.2(b)–(c) (requiring the appointment, registration and clearance through security risk assessment of a responsible official); 42 C.F.R. §§ 73.7–73.8; 9 C.F.R. §§ 121.6–121.8; 7 C.F.R. §§ 331.5–331.8 (requiring the entity to register, and to apply for and obtain approvals through the Attorney General's security risk assessment for, itself, any individual who will possess, use, ship or transfer listed agents or toxins, the responsible official, any alternate responsible official(s), and any individual who owns or controls the entity).

97. BPARA § 201(a), 116 Stat. at 642 (codified at 42 U.S.C.A. § 262a (2003)) (adding Section 351A(f) to the Public Health Service Act); § 212(e)(1), 116 Stat. at 649 (codified at 7 U.S.C.A. § 8401 (West Supp. 2003)); § 212(f), 116 Stat. at 652 (codified at 7 U.S.C.A. § 8401).

98. *Id.* § 201(a), 116 Stat. at 642 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(f) to the Public Health Service Act); § 212(f), 116 Stat. at 652 (codified at 7 U.S.C.A. § 8401); 42 C.F.R. § 73.16; 7 C.F.R. § 331.15; 9 C.F.R. § 121.16.

99. 42 C.F.R. § 73.9; 9 C.F.R. §§ 121.6(b)–(c), 121.10; 7 C.F.R. §§ 331.5(b)–(c), 331.9.

100. *See* 42 C.F.R. § 73.9; 9 C.F.R. §§ 121.6(b)–(c), 121.10; 7 C.F.R. §§ 331.5(b)–(c), 331.9; CDC FAQ, *supra* note 23.

101. BPARA § 201(a), 116 Stat. at 639 (codified at 42 U.S.CA. § 262a) (adding Section

individual to the Secretary and the Attorney General "promptly after . . . determining that such [individual needs] access" to listed agents or toxins, and again at intervals of at least every five years;[102] and (c) to deny access to listed agents and toxins to any individual identified by the Attorney General as a "restricted person" (as defined in Section 817(2) of the USA PATRIOT Act) and, if determined "appropriate" by the Secretary in consultation with the Attorney General, to deny or limit access to such agents and toxins to any individual identified by the Attorney General as "reasonably suspected by any Federal law enforcement or intelligence agency" of committing certain crimes relating to terrorism or knowing involvement with certain terrorist or violent organizations, or of being an agent of a foreign power under federal law.[103] The Attorney General is to promptly perform security risk assessments of entities and individuals whose names are submitted and to promptly notify the appropriate Secretary of the results.[104] The relevant Secretary is to determine whether registration is approved or denied and to promptly notify the entity and, if an individual's security risk assessment and registration are not approved, to promptly notify the individual.[105]

a. Registration Process: Submission of a Registration Application

The entity whose personnel or other individuals will use, possess, receive, or transfer listed, non-exempt agents or toxins must submit registration (including registration of the entity and grant of access for individuals) and security risk assessment applications on behalf of the entity, the Responsible Official, and Alternate Responsible Official(s), any individual who owns or controls the entity (subject to exclusions and limitations if the entity is an "accredited academic institution"), and all individuals who will possess, use, receive, or transfer listed agents or toxins. In rare cases where no entity is involved, the individual may submit these applications.

Before an entity submits its registration application or security risk assessment application containing individually identifiable information about faculty, students, and staff, it is important for the entity to determine whether there are any legal, contractual, or internal policy restrictions on the disclosure of such information, and if there are, for the entity to obtain appropriate consents to the disclosures from

351A(e)(2)(A) to the Public Health Service Act); § 212(e)(2)(A), 116 Stat. at 649 (codified at 7 U.S.C.A. § 8401).

102. *Id*. § 201(a), 116 Stat. at 639 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e)(2)(B) to the Public Health Service Act); 212(e)(2)(B), 116 Stat. at 649 (codified at 7 U.S.C.A. § 8401).

103. *Id*. § 201(a), 116 Stat. at 639 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e)(2)(C), (D) to the Public Health Service Act); § 212(e)(2)(C), 116 Stat. at 649 (codified at 7 U.S.C.A. § 8401).

104. *See id.* § 201(a), 116 Stat. at 639 (adding Section 351A(e)(3)(A) to the Public Health Service Act); § 212(e)(3)(A), 116 Stat. at 649–50 (codified at 7 U.S.C.A. § 8401); 42 C.F.R. § 73.8. The APHIS regulations are not as specific. 9 C.F.R. §§ 121.7(b), 121.8(a)–(b), (d), 121.11; 7 C.F.R. §§ 331.6(b), 331.7(a)–(c), 331.10.

105. BPARA § 201(a), 116 Stat. at 640 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e)(4) to the Public Health Service Act); § 212(e)(4), 116 Stat. at 650 (codified at 7 U.S.C.A. § 8401).

the affected individuals. As an employer, the institution is subject to its own policies, as well as to any applicable state common and statutory law governing privacy. Colleges and universities are also subject to the Family Education Rights and Privacy Act ("FERPA"),[106] governing the privacy of certain student records, as addressed in Part IV of this article.[107]

To satisfy FERPA's requirement that the affected student must consent before a college or university may disclose individually identifiable information about the student maintained by the institution (other than "directory information," the disclosure of which does not require a consent), the student must consent in writing and sign and date the consent, and the consent must identify the records to be disclosed, the purpose for disclosure, and to whom (person or categories of persons) disclosure will be made.[108] The FBI's security risk assessment form includes a broadly worded consent that must be signed by each individual, as addressed in Part III.A.4.b of this article, and this consent suffices for most purposes. Although the FBI's consent form allows any "individual" who has relevant information to disclose the information to any representative of the Justice Department, however, FERPA and other laws prohibit the *institution* from disclosing or permitting disclosure of certain individually identifiable information. Although the FBI's consent may arguably be read to cover an institution where an individual is acting on the institution's behalf, it may be prudent for the institution to develop its own consent form to supplement the FBI's form to make it clear that the consent reaches the institution. In addition, the institution should include in its transmittal letters submitting the registration and security risk assessment applications, that any information on students is being provided on the condition that the information will be used only for the purposes stated in the consent and will not be further disclosed without the affected students' consents.[109] See Part III.B.3 of this article for guidance on how to appropriately address these requirements.

106. Pub. L. No. 93-380, 88 Stat. 571 (1974) (codified as amended at 20 U.S.C.A. § 1232g (2000 & West Supp. 2003)) (note that FERPA's regulations are codified at 34 C.F.R. pt. 99.0 (2003)).

107. As part of the security risk assessment, the FBI or its contractors may contact the institution for information about individuals beyond what is included in the application forms, and additional laws may be implicated. For example, the FBI might ask an institution that has a hospital or medical department for its medical or mental health records on an individual. Any such request implicates HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996), and its regulations and standards, as well as similar state laws, and may implicate the institution's internal policies. *See supra* note 35 and accompanying text. *See also infra* Part III.B.3.

108. *See infra* Part IV; 20 U.S.C. § 1232g(b)(1), (b)(2)(A), (b)(4)(B) (prohibiting disclosure of "education records" without the affected student's consent with certain exceptions, and if consent is provided, requiring the institution to condition disclosure on the condition that the recipient will use the information only for the stated purpose and will not further disclose it without the affected student's consent), § 1232g(a)(4)(A)–(B) (defining "education records"); § 1232g(a)(5) (defining "directory information"), § 1232g(a)(5)(B) (permitting disclosure of directory information after notice of what is "directory" and an opportunity to "opt out," without consent); § 1232g(d) (providing for college students to exercise consent rights otherwise given parents).

109. *Id.*

To begin the process, the entity submits an application for registration and requests a registration identification number from the CDC or APHIS, as applicable.[110] Where overlap agents or toxins are concerned, the entity may submit an application either to the CDC on its Form 0.1319 or to APHIS on its Form 2044, and the two agencies will confer and agree before one approves or denies the registration of the entity and grants access for individuals on behalf of both agencies.[111] Otherwise, the entity submits the form to the agency whose regulations apply, the CDC for HHS agents and toxins and APHIS for USDA animal or plant agents and toxins.[112]

Although the issue has not been decided by a court, it is a reasonable interpretation of the regulations to conclude that a landlord need not register if its tenant will be undertaking activities with listed, non-exempt agents or toxins, but should require its tenant to do so in order to operate in the leased premises in accordance with applicable laws. The regulatory requirements are expressly directed to entities that undertake activities, not to entities that merely own facilities used by other entities for these activities. Also, the individuals for whom an entity must submit registration and security risk assessment applications are the individuals who are responsible to, employed by, or acting on behalf of, the entity. Employees of a tenant entity would not typically be acting on behalf of the landlord entity in undertaking work with agents or toxins.[113]

The application forms request, among other information, the (a) name, address, type, and contact information for the entity; (b) name, source, and, if available to the applicant, information characterizing the agent and toxin and quantities held, if any, at the time of application; (c) the location, with building and room identifiers and floor plans, where a listed, non-exempt select agent or toxin will be stored or used; (d) information (in the case of CDC) and copies (in the case of APHIS) of safety, security, emergency response, and training plans, satisfying the other provisions of the regulations; (e) name, address, title, and identification information (social security number and date of birth) of the Responsible Official and any Alternate Responsible Official(s); (f) the names, titles, addresses, and identification information (social security number and date of birth) of all individuals who will need unescorted access to the listed, non-exempt agents or toxins; (g) the Responsible Official's certification of authority to bind the entity

110. 42 C.F.R. § 73.7(b). APHIS' regulations are not as detailed as CDC's, but APHIS generally follows the same process and uses the same application form, issued under a joint CDC/APHIS letter, *available at* http://www.cdc.gov/od/sap/downloads2.htm (last visited Apr. 4, 2004). The agencies provide a registration number after the registration application is submitted and the security risk assessment application and fingerprint cards are submitted, although this sequence may change over time as CDC, APHIS, and the FBI work through the implementation and coordination of their respective processes.

111. 42 C.F.R. § 73.7(c), (e); 9 C.F.R. §§ 121.7(c), 121.9(c) (2004).

112. 42 C.F.R. § 73.7(c), (e); 9 C.F.R. §§ 121.7(c), 121.9(c).

113. *See* 42 C.F.R. § 73.7 (referring to the entity's obligations to submit a registration application on behalf of the entity, individuals who own or control the entity, the entity's Responsible Official, and individuals who will need access to regulated agents and toxins); 42 C.F.R. § 73.9 (requiring the Responsible Official to be an individual who is authorized to act on behalf of the entity).

and compliance with the regulatory requirements; and (h) "[a]ny other information necessary for the determination."[114] Thus, the Secretaries have broad discretion to require a wide range of information in the registration process.

Although the regulations and forms do not address what is meant by the Responsible Official having authority to bind the institution, it is reasonable to interpret this certification (which is the same certification as was included in the registration application under the AEDPA's regulations) to mean that the Responsible Official must be authorized to bind the entity in connection with the biological agent and toxin program. A senior officer of the institution with the appropriate authority should designate the institution's Responsible Official and Alternate Responsible Official, and should authorize these individuals to act on behalf of the institution in connection with the agent and toxin program under the BPARA before the registration application is submitted.

b. Security Risk Assessment Process: Submitting an Application

The appropriate Secretary's approval of an entity's application for registration of the entity and, for a grant of access for the relevant individuals to possess, use, transfer, receive, and have access to listed, non-exempt agents or toxins must depend in part on such entity's and individuals' security risk assessment approval by the Attorney General.[115] The BPARA requires the Attorney General, "[u]pon receipt of names and other identifying information" about individuals who require access to listed agents and toxins, to "promptly use criminal, immigration, national security, and other electronic databases that are available to the Federal Government and are appropriate" for the "sole purpose of identifying whether the individual[] involved" is a "restricted person" under the USA PATRIOT Act or is "reasonably suspected by any Federal law enforcement or intelligence agency" of committing certain federal crimes relating to terrorism or knowing involvement with certain terrorist or violent organizations, or being an agent of a foreign power under federal law.[116] The Attorney General must promptly, after receiving the individual's or entity's name, undertake this background check and notify the appropriate Secretary of whether any individual whose name has been submitted or the entity fall under any of these categories.[117] The Secretary must then "promptly notify" the entity involved of whether any such individual or the entity is denied access to listed, non-exempt agents and toxins (which must occur in connection with any individual who is a "restricted person" under the USA PATRIOT Act),

114. 42 C.F.R. § 73.7(b). *See also* CDC Form 0.1319, *available at* http://www.cdc.gov/od/sap/downloads2.htm (last visited Apr. 4, 2004), 9 C.F.R. §§ 121.7, 121.9; APHIS Form 2044, *available at* http://www.cdc.gov/od/sap/downloads2.htm (last visited Apr. 4, 2004); 7 C.F.R. § 331.6, 331.8.

115. *See* 42 C.F.R. § 73.8(a); 9 C.F.R. §§ 121.6, 121.8(a); 7 C.F.R. §§ 331.6, 331.7(a).

116. BPARA § 201(a), 116 Stat. 594, 639–40 (codified at 42 U.S.C.A. 262a (2003)) (adding Section 351A(e)(3) to the Public Health Service Act); § 212(e)(3), 116 Stat. at 649–50 (codified at 7 U.S.C.A. § 8401 (West Supp. 2003)).

117. *Id*. § 201(a), 116 Stat. at 639–40 (codified at 42 U.S.C.A. 262a) (adding Section 351A(e)(3)(C) to the Public Health Service Act); § 212(e)(3)(C), 116 Stat. at 650 (codified at 7 U.S.C.A. § 8401).

and if denied access, must notify the individual as well.[118] Subject to certain phase-in provisions of the regulations that no longer apply, an entity may not provide access to such agents or toxins, and individuals must not access such materials, unless and until the entity and individuals are either finally or provisionally approved by the Secretaries based on the security risk assessment.[119]

The FBI conducts security risk assessments for the Attorney General and has issued an application form and accompanying fingerprint cards for this purpose.[120] An updated guidance on security risk assessment applications, issued in August 2003 by the CDC, provides that these applications and fingerprint cards must be submitted to the FBI directly, not to the CDC or APHIS as had been indicated in the FBI's earlier instructions on the application form.[121]

The entity and the Responsible Official, Alternative Responsible Official(s), any individual who will possess, use, receive, transfer, or have unescorted access to listed, non-exempt agents or toxins, and, with limited exceptions, any individual who owns or controls the entity, must complete the security risk assessment application form, are subject to a full assessment, and all such individuals must

118. *Id*. § 201(a), 116 Stat. at 640 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e)(4) to the Public Health Service Act); § 212(e)(4), 116 Stat. at 650 (codified at 7 U.S.C.A. § 8401).

119. *See supra* notes 94–96, 101–103 and accompanying text. An interim final rule became effective on November 3, 2003, under which the CDC and APHIS were authorized to issue "provisional registration certificates" to those entities and "provisional grants of access" to those individuals who, by November 12, 2003, submitted to the Attorney General through the FBI complete security risk assessment applications and fingerprints but whose applications were not acted upon by that date, whose applications for registration and access approval are pending with CDC or APHIS, as applicable, and whose applications otherwise satisfy all of the regulatory requirements. Agricultural Bioterrorism Protection Act of 2002: Possession, Use, and Transfer of Biological Agents and Toxins, 68 Fed. Reg. 62,218–62,219 (Nov. 3, 2003). Upon receiving provisional registration or grant of access, an entity and individual who meet all of the requirements of the BPARA regulations, other than completing the security risk assessment process, may continue or begin to possess and use regulated agents and toxins. *Id.* The CDC explains that the provisional registration and grant of access are necessary "to ensure that both ongoing and new research and educational efforts important to the national defense are not disrupted." CDC, Additional Information on the Interim Final Rule, Nov. 3, 2003, *at* http://www.cdc.gov/od/sap/ifr-info.htm. In so doing, the CDC recognizes that the FBI can process about 1,200 security risk assessment applications per month, but had 4,600 applications to process as of early November 2003 and would not complete these by the November 12, 2003, deadline for full implementation of the BPARA regulations. *Id.*

120. *See* CDC, Security Risk Assessment (Aug. 2003) (updated instructions on the security risk assessment process and its coordination with the registration process), *at* http://www.cdc.gov/od/sap/securisk.htm [hereinafter CDC Security Risk Assessment]; FBI, Criminal Justice Information Services Division, *available at* http://www.fbi.gov/hq/cjisd/cjis.htm (last visited Apr. 4, 2004) (FBI fingerprint instructions); FBI, Bioterrorism Preparedness and Response Act FBI Information Form (Form FD-961), *available at* http://www.fbi.gov/terrorinfo/bioterrorfd961.htm (last visited Apr. 4, 2004) [hereinafter FBI Form FD-961] (application for security risk assessment under the BPARA and related instructions). The FBI's instructions on Form FD-961 have not been updated, and should be read in conjunction with the updated guidance and fingerprint instructions. *See infra* Parts III.B and IV, and *supra* Part III.A.4.a.

121. *See id.*

complete fingerprint cards.[122] The CDC's updated guidance on the process provides for the individual to submit his or her portion of the application form directly to the FBI, although many entities' Responsible Officials assemble the applications for all of the relevant individuals associated with the entity and submit them in one package in order to ensure that the applications are timely and properly submitted.[123]

"Entity" for purposes of the security risk assessment is broadly defined in the regulations and in instructions to the FBI form to include "any government agency (Federal, State or local), academic institution [or university], corporation, company, partnership, society, association, firm, sole proprietorship, or other legal entity[, including an individual acting on his or her own]."[124] Although they are included in the definition of "entity," local, state, and federal agencies, including public academic institutions, and anyone who "owns" them, are not subject to the security risk assessment requirement.[125] The regulations and application form and instructions, however, draw an important distinction between the government agency (the entity), which is not subject to the security risk assessment requirement, and such agency's Responsible Officials, Alternate Responsible Officials, and other individuals with access to regulated agents or toxins or working for or acting on behalf of such agency, who are subject to this requirement.[126] Consequently, any state college or university is not itself subject to the security risk assessment process, but its personnel are; and a state college or university must complete a portion of the security risk assessment application for purposes of clearing its personnel through the process.[127]

The FBI form has a number of sections. The entity must complete the first section, including the entity's legal name, address, and type (i.e., academic, commercial, government, private, or other).[128] Although a government agency, including a state college or university, is not subject to the security risk assessment process, the state institution should complete the first section of the application form and check "government" and "academic" for identification purposes in connection with the agency's individuals' applications for security risk assessment approval.[129] Other colleges and universities should check "academic."[130]

The regulations provide that any individual who "owns or controls" an entity is

122. CDC Security Risk Assessment, *supra* note 120.

123. *See supra* note 120. The entity must take steps to ensure that it is not violating any laws, contracts, or internal policies relating to disclosure of individually identifiable information about individuals. *See supra* note 35 and accompanying text.

124. 42 C.F.R. § 73.1 (2003); 9 C.F.R. § 121.1 (2004); 7 C.F.R. § 331.1 (2004).

125. *See* 42 C.F.R. § 73.8(a), (c); 9 C.F.R. § 121.7(b), n.7; 7 C.F.R. § 331.6(b), n.4; FBI Form FD-961, *supra* note 120; CDC Security Risk Assessment, *supra* note 120 ("if the entity is a local, state, or federal institution, then the owners do not require a security risk assessment"). *Id*.

126. See 42 C.F.R. § 73.8(a), (c); 9 C.F.R. § 121.7(b), n.7; 7 C.F.R. § 331.6(b), n.4; FBI Form FD-961, *supra* note 120; CDC Security Risk Assessment, *supra* note 120.

127. FBI Form FD-961, *supra* note 120; CDC Security Risk Assessment, *supra* note 120.

128. FBI Form FD-961, *supra* note 120.

129. *See id.*

130. *See id.*

subject to the security risk assessment process.[131] This requirement, and section II of the FBI form which addresses it, have created a great deal of confusion about the meaning of ownership or control of an entity for purposes of the BPARA, particularly in connection with government agencies and academic institutions.

The FBI has determined that anyone who "owns" a government agency is not subject to security risk assessment, and the regulations exclude the agency itself from assessment, as discussed above.[132] Presumably, this means that a government agency and its owners need not complete the portion of section II of the FBI's application form that requests the names of, and other identifying information about, the agency's owners, and that any such owners need not complete fingerprint cards. (It is unclear how any individual could own a government agency in any event; however, the updated guidance on the security risk assessment process seems to assume there may be owners, but they are exempted from the process.) The Responsible Official, Alternate Responsible Official, and individuals with access to regulated agents and toxins are subject to security risk assessments and presumably, based on the regulatory requirements, so are the individuals who control the agency for purposes of overseeing the agency's regulated agent and toxin program, although the updated guidance and instructions for the security risk assessment application are silent on this point.[133] The individuals with control of the agency for this purpose may be the Responsible Official and Alternate Responsible Official, or may also include all of the agency's leaders, from those who oversee laboratories that use regulated agents and toxins through the chain of command up to the agency head.[134] The agency should note in section II of the FBI's form that information on the Responsible Official and Alternate Responsible Official is provided in sections III and IV of the form, although the agency itself is not subject to security risk assessment under the regulations.[135] The agency should also either provide the requested information on officials in the chain of command overseeing the agency's regulated agent and toxin uses, or explain why the Responsible Official and Alternate Responsible Official are the only officials with control of the agency for this purpose.[136]

131. 42 C.F.R. § 73.8(a), (c) (2003); 9 C.F.R. § 121.7(b), n.7 (2004); 7 C.F.R. § 331.6(b), n.4 (2004).

132. *See* 42 C.F.R. § 73.8(a), (c); 9 C.F.R. § 121.7(b), n.7; 7 C.F.R. § 331.6(b), n.4; FBI Form FD-961, *supra* note 120; CDC Security Risk Assessment*, supra* note 120 ("if the entity is a local, state, or federal institution, then the owners do not require a security risk assessment"). *Id.*

133. *See* CDC Security Risk Assessment*, supra* note 120; FBI Form FD-961, *supra* note 120.

134. *Cf.* Letter from David Hardy, Chief, Records/Information Dissemination Section, FBI, to Tony DeCrappeo, Associate Director, Council on Government Relations (Apr. 4, 2004) [hereinafter Hardy Letter] (concerning a similar issue relating to those who control academic institutions for purposes of the security risk assessment process). For a copy of the letter from DeCrappeo to Hardy and the letter from Hardy responding to DeCrappeo, visit The Journal of College and University Law, Symposium Webpage, Appendix D, *available at* http://www.nd.edu/~jcul/USA_PATRIOT_Act/Appendix_D.pdf (last visited Apr. 4, 2004).

135. FBI Form FD-961, *supra* note 120.

136. *See* CDC Security Risk Assessment*, supra* note 120 (clarifying that the "owners" of government agencies need not apply for security risk assessments and that only such agencies

The FBI initially determined in its instructions on the security risk assessment application form that private academic institutions must complete all of section II, but later amended its determination to exclude "owners" of "accredited academic institutions" from the security risk assessment requirement.[137] Consequently, it should not be necessary for such an institution to list "owners" (defined in the form and updated guidance, as stockholders holding 50% or more of the entity's "voting stock" who are in "managerial or executive capacity[ies for] agent[s and toxins] possessed, used, or transferred by the entity") in section II of the application form.[138] This is sensible, as private academic institutions are often non-profit organizations under state and federal law, and as such do not have stockholders or similar "owners."[139] Such organizations are prohibited by the Internal Revenue Code, and often by state law, from operating for the benefit of any individuals, and instead operate for the benefit of their charitable purposes.[140]

In addition to owners, section II of the FBI form requests the names, dates of birth, and social security numbers of the "corporate officers/entity leadership" and the "board of directors (if applicable)."[141] These appear to be officials who control the entity. The FBI ultimately limited its definition of who "controls" an accredited academic institution for purposes of the security risk assessment, to the institution's "responsible official" for regulated agent and toxin activities.[142] The FBI determined that the "responsible official with regard to the select agent [or toxin] possessed, used, or transferred by the entity" is the person who controls the entity for security risk assessment purposes.[143] The Responsible Official and Alternate Responsible Official must be authorized to bind the institution in connection with, and are the individuals who are responsible for, regulated agents and toxins at the institution,[144] and consequently, an accredited private academic institution should note in section II that the Responsible Official and Alternate Responsible Official control regulated agent and toxin activities at the institution, and their information is included in sections III and IV of the form.[145] The institution arguably may not be required to list anyone else in section II.

In an unpublished April 2003 letter, a copy of which is included in Appendix

Responsible Officials, Alternate Responsible Officials, and individuals with access to regulated agents and toxins must apply for such assessments and, consequently, indicating that there is no requirement for anyone who "owns" the government agency to apply for a security risk assessment or implicitly determining that there is no such person).

137. *Id*.

138. *Compare with* FBI Form FD-961, *supra* note 120. The FBI's instructions on the form have not been updated as of the date this article went to the printer.

139. *See* BRUCE R. HOPKINS, THE LAW OF TAX-EXEMPT ORGANIZATIONS 4–5 (8th ed. 2003).

140. *See id*.

141. FBI Form FD-961, *supra* note 120.

142. CDC Security Risk Assessment, *supra* note 120.

143. *Compare id. with* FBI Form FD-961, *supra* note 120, at Part II, additional instruction 3, *and* Hardy Letter, *supra* note 134.

144. *See infra* part III.A.4 and *supra* note 105; 42 C.F.R. § 73.9 (2003); 9 C.F.R. §§ 121.6(b), 121.10 (2004); 7 C.F.R. §§ 331.5(b), 331.9 (2004); CDC FAQ, *supra* note 23.

145. FBI Form FD-961, *supra* note 120.

D[146] to this article, however, the FBI advises academic institutions to list all officials in the chain of command overseeing regulated agent and toxin activities, from the laboratory head to the President, in section II of the application form.[147] The letter also acknowledges that an academic institution need not list its entire board and may list the "principal members" or the "separate board," or presumably committee of the board, with oversight of select agent and toxin activities.[148] While the letter states that such persons in control of the institution for security risk assessment purposes, who do not also have access to agents and toxins, do not have to complete the full application, and do not have to complete fingerprint cards, the updated guidance states that all individuals who "own or control" an entity must complete the application and fingerprint cards.[149] A very good argument exists that since this non-binding letter was written, (1) the FBI decided (and CDC published a guidance) to define the criteria for those who "control" an accredited academic institution for security risk assessment purposes in the same way as the CDC and APHIS define the responsibilities of the Responsible Official and Alternate Responsible Official; (2) the Responsible Official and Alternate Responsible Official have to complete the full application and fingerprint cards (as the FBI has determined all individuals who control the entity must do); and, consequently, (3) as a general rule, the Responsible Official and the Alternate Responsible Official will be deemed to "control" the institution for security risk assessment purposes, and an accredited academic institution need not list anyone else in section II of the form.[150] In any event, the institution should explain in section II why it is listing those it lists and not others. Accredited academic institutions are "[p]ostsecondary, language or vocational schools . . . accredited by an accrediting agency recognized by the United States Department of Education."[151]

Responsible Officials, Alternate Responsible Officials, and individuals who will have unescorted access to listed, non-exempt agents or toxins must complete Sections III and IV of the FBI form.[152] Section III asks for personal information to assist the FBI in identifying the individual (e.g., name, date of birth, social security

146. *See* Hardy Letter, *supra* note 134.

147. *Id.*

148. *Id.*

149. *Id.*

150. Under the earlier informal FBI guidance (e.g., Hardy Letter, *supra* note 134; FBI Form FD-961, *supra* note 120), private academic institutions are required to complete Section II of the application and to list the chain of command at the institution overseeing agent and toxin activities from the laboratory to the president. These instructions have not been updated, and read in conjunction with the updated guidance, may require academic institutions to list in section II of the security risk assessment form both the responsible official for activities involving the agents and toxins being registered (the Responsible Official and any Alternate Responsible Official) and the officials in the chain of command in charge of the laboratory up to the President. There is great variation in the way institutions have interpreted this requirement, and some explanation of why an institution is interpreting the requirement in a particular way should be provided to the FBI with section II of the application.

151. *See* CDC Security Risk Assessment, *supra* note 120.

152. FBI Form FD-961, *supra* note 120.

number, and residential address).[153] The form also asks for racial and citizenship information and the individual's entity affiliation.[154] Finally, after admonishing individuals that "falsifying or concealing a material fact is a felony," the form enumerates the criteria for a "restricted person" under Section 817(2) of the USA PATRIOT Act and requires the individual to reply "yes or no" as to whether each criterion applies.[155] Section IV is a very broad consent form with a Privacy Act Statement attached that the individual must sign.[156] The individual must (a) consent to the Justice Department acquiring information "relevant to assessing my suitability to access, possess, use, receive or transfer select biological agents and toxins from any relevant source . . . includ[ing] but not limited to . . . biographical, financial, law enforcement and intelligence information," (b) authorize "any individuals having information pertinent to such an assessment to release such information to a duly accredited representative of the U.S. Department of Justice," (c) authorize the release of information and records "relating to, or obtained in" the security risk assessment process to any law enforcement or intelligence authority or any federal, state, or local entity "with relevant jurisdiction where such information reveals a risk to human, animal and/or plant health or national security," (d) authorize disclosure of information and records "relating to or obtained in" the security risk assessment process to public and private organizations and individuals "if deemed necessary, in the sole discretion of the U.S. Department of Justice, to elicit information or cooperation from the recipient for use in assessing my suitability to access, possess, use, receive, or transfer select biological agents and toxins," (e) authorize release of information and records "relating to or obtained in" the security risk assessment process to public or private "laboratories, universities, individuals, or other entities . . . responsible for making security assessments, employment and/or licensing determinations and suitability or security decisions when the information is relevant to an assessment of my suitability to access, possess, receive, use, or transfer biological agents or toxins."[157] The accompanying Privacy Act statement discloses that the information obtained in the process is to be used primarily for the security risk assessment.[158] The Privacy Act statement, however, provides that information obtained in the process may be provided to a wide range of public and private individuals, entities, and agencies "charged with the responsibility of investigating, prosecuting, and/or enforcing laws, regulations . . . or contracts if any part of the information [alone or together with other information] indicates a violation or potential violation of law, regulation . . . or contract," among other broad uses and for any "routine uses most recently published in the Federal Register for the FBI."[159] If one considers the broad range of criteria defining a "restricted person" under Section 817(2) of the USA PATRIOT Act and the broad terms of the

153. *Id.*
154. *Id.*
155. *Id.*
156. *Id.*
157. *Id.*
158. *Id.*
159. *Id.*.

consent form and Privacy Act statement, the effect of this consent, which is mandatory for any individual who seeks a security risk assessment approval, is that a broad range of information about the individual may be obtained, disclosed, or used for many FBI, Justice Department, law enforcement, and national security purposes, and even in connection with private contracts.[160] In addition to the application form, fingerprint cards, which must be obtained from the FBI, must be completed by all individuals who are subject to the security risk assessment process with a law enforcement agency (that may be the campus police if they are sworn law enforcement officers under state law), and must be returned to the FBI with the security risk assessment application.[161]

The standard for security risk assessment approval is (a) whether the individual is a "restricted person" under Section 817(2) of the USA PATRIOT Act, in which event the Attorney General will not approve the individual's security risk assessment, and the Secretaries must deny or revoke the individual's application for access approval[162] or (b) whether the individual is "reasonably suspected by any Federal law enforcement or intelligence agency of" (i) "[k]nowing involvement with an organization that engages in domestic or international terrorism (as defined in 18 U.S.C. § 2331)[163] or with any other organization that engages in intentional crimes of violence;" or (ii) "[b]eing an agent of a foreign power as defined in 50 U.S.C. § 1801" (the Foreign Intelligence Surveillance Act ("FISA")),[164] in which event the relevant Secretary must confer with the Attorney General and then decide whether to deny or limit access to select agents and toxins by such individual or whether there is a national security, public health, or safety,

160. Some have raised the question of whether this consent form and the broad acquisition and use of information required by the Justice Department and FBI to be authorized, exceed the authority of the Justice Department or FBI or otherwise constitute an abuse of their discretion. One might argue, for example, that completion of the FBI consent form is a condition of registration and, consequently, the consent is not voluntary. The government would likely respond that an individual does not have the right to work with listed biological agents and toxins in the absence of approval through the security risk assessment process required by Congress and is not compelled to work with such agents and toxins. Another argument would be that the permissible uses of the information as described in the FBI form exceed the authority granted to the FBI in the statute. The government might reply that the uses are permitted under the Privacy Act's "routine uses" exception, which allows the government to disclose information "for a purpose which is compatible with the purpose for which it was collected" if "each routine use of the records [is published in the Federal Register]." 5 U.S.C. § 552a(b)(3) (2000). Although these questions have not been decided by the courts, in the current environment and in light of the broad authority and discretion of the Justice Department and FBI, there is likely to be a heavy burden on anyone who seeks to challenge the requirement for this consent form or the related authorization to secure and use information. In any event, an individual will not have access to regulated agents or toxins until the challenge is resolved and a security risk assessment is completed.

161. FBI Form FD-961, *supra* note 120 (stating that Responsible Officials should not wait for fingerprint cards before submitting security risk assessment applications). The FBI subsequently changes its policy to require that fingerprint cards be submitted with the application. CDC Security Risk Assessment*, supra* note 120.

162. 42 C.F.R. § 73.8(d)–(e) (2003); 9 C.F.R. § 121.8(a) (2004); 7 C.F.R. § 331.7(a) (2004).

163. *See* 42 C.F.R. § 73.8(d)–(e); 9 C.F.R. § 121.8(a); 7 C.F.R. § 331.7(a).

164. *See* 42 C.F.R. § 73.8(d)–(e); 9 C.F.R. § 121.8(a); 7 C.F.R. § 331.7(a).

or protection of animal or plant health or products reason not to do so.[165] A security risk assessment approval is valid for five years, unless the relevant Secretary terminates it sooner.[166]

c. Completing the Registration Process and Effectiveness of Registration

The Secretary of HHS or Agriculture will approve an application for registration if the activities involving listed, non-exempt agents or toxins are "lawful," the entity and individuals are approved in the security risk assessment process, and all of the regulatory requirements (e.g., for security, training, safety, record-keeping, emergency preparedness and response) are met.[167] Approval is evidenced by the issuance of a certificate of registration that is valid for up to three years (unless earlier terminated) and covers only the agents or toxins, the activities using them, and the locations that are specified in the application.[168] The CDC's regulations provide that a single location may include "a building or complex of buildings at a single mailing address."[169]

The Secretary of HHS or Agriculture *must* deny an application for approval of access to select agents of an individual who is a restricted person under the USA PATRIOT Act, as determined by the U.S. Attorney General's security risk assessment,[170] if the activities involving the regulated agents or toxins are not "lawful,"[171] or if the other requirements of the regulations are not met.[172] After consulting with the Attorney General, the Secretary will deny an application for access of an individual who is determined in such security risk assessment to fall under any of the other categories for denial of security risk assessment approval, or may approve or limit access to listed non-exempt agents and toxins by such individual, as warranted by the public health or safety, national security, or to protect animal or plant health or products.[173]

The relevant Secretary may terminate a certificate of registration for failure to comply with the regulations or if the Secretary determines that it is necessary to do so to protect the public health or safety (in the case of HHS or overlap agents and toxins) or to protect animal or plant health or products (in the case of USDA or overlap agents and toxins).[174] The Secretaries will terminate a certificate of

165. 42 C.F.R. § 73.7(e). *See* 9 C.F.R. § 121.8(a)(2); 7 C.F.R. § 331.7(a)(2).

166. 42 C.F.R. § 73.8(f); 9 C.F.R. § 121.11(k); 7 C.F.R. § 331.10(j).

167. *See* 42 C.F.R. § 73.7(e); 9 C.F.R. § 121.7(b)–(c); 7 C.F.R. § 331.6(b).

168. 42 C.F.R. § 331.6(c), (f); 7 C.F.R. § 73.7(d), (g); 9 C.F.R. § 121.7(d), (g).

169. 42 C.F.R. § 73.7(f). A campus may be one location for registration purposes. A college and university that has multiple campuses or locations, such as in different municipalities or in distinct parts of the same municipality, however, would need separate registrations for each campus or location.

170. 42 C.F.R. § 73.8(e). *See* 9 C.F.R. § 121.8(a)(1); 7 C.F.R. § 331.7(a)(1).

171. 7 C.F.R. § 331.7(a)(3); 9 C.F.R. § 121.8(a)(3). *See* 42 C.F.R. § 73.7(e).

172. 7 C.F.R. § 331.7(a)(4)–(6); 9 C.F.R. 121.8(b)(4)–(6). *See* 42 C.F.R. § 73.7(e).

173. 42 C.F.R. § 73.8(e); 9 C.F.R. § 121.8(a)(2), (a)(7), (b); 7 C.F.R. 331.7(a)(2), (a)(7).

174. 42 C.F.R. § 73.8(f); 9 C.F.R. § 121.8(a)(3)–(7), (b); 7 C.F.R. § 331.7(a)(3)–(7).

registration upon the cessation of activities covered by the certificate.[175] Some institutions have been accustomed to maintaining their registrations under the regulations implementing the AEDPA, even when covered agents or toxins are no longer at the institution or when their transfer to the institution never occurred as planned, in order to be able to accommodate the quickly changing needs of faculty who are doing biological research and who may need to acquire regulated agents or toxins. The BPARA and its regulations make clear that this is not permissible any longer, and institutions must notify the appropriate Secretary through CDC or APHIS, when registered agents or toxins or activities cease.[176] The entity's Responsible Official must "immediately" (in the case of USDA agents or toxins) and "promptly" (in the case of HHS agents or toxins) notify the relevant Secretary if there is a change in any of the information provided in the registration process, and the certificate of registration must be amended before most changes occur.[177] Changes include, without limitation, additions or deletions of individuals who must be approved through the security risk assessment process (e.g., the Responsible Official and individuals who will have unescorted access to listed non-exempt agents or toxins), changes in the activities involving such agents or toxins, changes in the "protocols or objectives of the studies" using such agents or toxins, changes in ownership or control of the entity, and changes in the locations where the work will occur.[178]

Upon termination of a certificate of registration, the entity must appropriately destroy the related agents or toxins.[179] Entities are required to notify the Secretary of HHS through the CDC or the Secretary of Agriculture through APHIS, as applicable, at least five business days before destroying a listed, non-exempt agent or toxin "for the purpose of discontinuing activities with a select agent or toxin covered by a certificate of registration" and the Secretary may "observe the destruction or take other action as appropriate" and must terminate or amend the

175. 42 C.F.R. § 73.7(d), (h). *See* 9 C.F.R. §§ 121.7(d), 121.8; 7 C.F.R. §§ 331.6(c), 331.7.

176. 42 C.F.R. § 73.7(d); 7 C.F.R. § 331.6(d); 9 C.F.R. § 121.7(e).

177. 42 C.F.R. § 73.7(d); 9 C.F.R. § 121.7(e); 7 C.F.R. § 331.6(d). *See* CDC FAQ, *supra* note 23. Presumably, it would be impossible under some circumstances to receive pre-approval of the change that gives rise to an amended certificate of registration, such as when the amendment is necessary to remove a registered individual who is leaving the institution.

178. 42 C.F.R. § 73.7(d); 9 C.F.R. § 121.7(e); 7 C.F.R. § 331.6(d). *See* CDC FAQ, *supra* note 23. When there are changes concerning any of the individuals who require security risk assessments, CDC's updated guidance on coordination of the registration and security risk assessment processes provides instructions on how to process this change. The entity's Responsible Official updates table 4B of CDC's or APHIS' registration application form, as applicable, and submits it to the agency. The agency obtains a "unique identifying number" for the new individual from the Attorney General through the FBI and provides it to the entity's Responsible Official in a letter. The entity should then oversee the individual's completion of the FBI's security risk assessment application, form FD-961, insertion of the unique identifier, and completion of fingerprint cards. The form is then sent to the FBI for processing. The entity must ensure that the first two sections of the form are completed and the individual completes sections III and IV. *See* CDC Security Risk Assessment, *supra* note 120; FBI Form FD-961, *supra* note 120.

179. 42 C.F.R. § 73.7(h); 9 C.F.R. § 121.7(f); 7 C.F.R. § 331.6(e).

certificate of registration accordingly.[180]

Neither the BPARA, nor CDC's or APHIS' regulations, specify a deadline by which CDC or APHIS must process a registration application or by which the Attorney General must process a security risk assessment application, although the Attorney General is required to act "promptly" after receiving the necessary information and the CDC and APHIS are required to give "prompt notice" of a registration decision to the entity, and to the individual if the individual's application is denied, once the agency receives the results of the Attorney General's security risk assessments.[181] The initial registration process in 2003 and early 2004 took over nine months for most institutions.[182] The Secretary may request "expedited review" by the Attorney General when the applicant "demonstrates good cause,"[183] although the utility of this provision is questionable unless the regular registration process becomes significantly more efficient. The flood of registration requests was greatest in the first year of the regulations' implementation because so many existing activities were captured by the registration requirement. It is probably reasonable to expect that the demand for registration will be significantly less for a time after the initial registrations are processed. Institutions, however, are cautioned that the initial registration certificates issued in 2003 or early 2004 will expire on or about the same time in 2006 or early 2007, likely producing another flood of applications, this time for renewals of registrations.[184]

An entity may obtain review by the Secretary of HHS or USDA of the denial or revocation of the entity's registration, and an individual may obtain such review of the denial of the individual's access to listed, non-exempt agents or toxins.[185] The request for review must be made in writing within thirty days of the Secretary's

180. 42 C.F.R. § 73.7(h); 9 C.F.R. § 121.7(f); 7 C.F.R. § 331.6(e).

181. BPARA § 201(a), 116 Stat. 594, 640 (codified at 42 U.S.C.A. § 262a (2003) (adding Section 351A(e)(3)(C), (e)(4), (e)(6) to the Public Health Service Act); §§ 212(e)(3)(C), 212(e)(4), 212(e)(6), 116 Stat. at 649–51 (codified at 42 U.S.C.A. § 8401 (West Supp. 2003)); 42 C.F.R. § 73.8(c).

182. The author participated on a Council on Government Relations Task Force on Bioterrorism that tracked member colleges' and universities' registration progress. The Secretary of Health and Human Services provided for provisional registration when it became clear that the registration process could not be completed for many applicants by the November 12, 2003, full implementation deadline eleven months after the regulations under the BPARA were promulgated. *See supra* note 119.

183. BPARA § 201(a), 116 Stat. at 640 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e)(5) to the Public Health Service Act); § 212(e)(5), 116 Stat. at 650 (codified at 42 U.S.C.A. § 8401); 42 C.F.R. § 73.8(g); 9 C.F.R. § 121.11(f); 7 C.F.R. § 331.10(f) (all of the regulations provide that good cause for expedited review includes "public health or agricultural emergencies, national security, impending expiration of a research grant, [and] a short-term visit by a prominent researcher").

184. *See* 42 C.F.R. § 331.6(f); 7 C.F.R. § 73.7(g); 9 C.F.R. § 121.7(g) (a certificate of registration is valid for up to three years).

185. BPARA § 201(a), 116 Stat. at 641 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e)(7) to the Public Health Service Act); § 212(e)(7), 116 Stat. at 651 (codified at 42 U.S.C.A. § 8401; 42 C.F.R. § 73.18; 9 C.F.R. §§ 121.8(e), 121.18; 7 C.F.R. §§ 331.7(d), 331.17.

adverse action.[186] The Secretary may conduct an *ex parte* review of relevant information when disclosure of the information "could compromise national security or an investigation by any law enforcement agency" and the Secretary may, alternatively, "substitute a summary of the information to which the person may respond."[187] The Secretary's decision in such review constitutes final agency action under the Administrative Procedures Act[188] and the aggrieved individual or entity may appeal the Secretary's decision to federal court.[189] The court's review also may be *ex parte* if disclosure of information "could compromise national security or an investigation by any law enforcement agency."[190] The government may avail itself of interlocutory appeal and expedited consideration under 18 U.S.C. §§ 2339B(f)(5)(A) and (B)(i) if a court authorizes disclosure of information that the government "believes could compromise national security or an investigation by any law enforcement agency."[191]

5. Security Requirements

The BPARA requires that there be adequate security for listed, non-exempt agents and toxins, and provides that the required security must be commensurate with the risk posed by the agent or toxin, allowing security requirements to differ in accordance with differing levels of risk posed by particular agents and toxins.[192] The regulations' baseline security and related record-keeping requirements, however, are among the most prescriptive and burdensome of the regulatory requirements.[193] An entity must develop and implement a security plan that identifies threats, examines and mitigates vulnerabilities, and employs a systematic approach to security, covering the areas in a building where regulated agents or toxins are used or stored, as well as such materials' containers.[194] The entity must

186. 42 C.F.R. § 73.18; 9 C.F.R. § 121.18; 7 C.F.R. § 331.17.

187. BPARA § 201(a), 116 Stat. at 641 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e)(7) to the Public Health Service Act); § 212(e)(7), 116 Stat. at 651 (codified at 42 U.S.C.A. § 8401).

188. 5 U.S.C.A. § 702 (1996 & West Supp. 2003).

189. BPARA § 201(a), 116 Stat. at 641 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e)(7) to the Public Health Service Act); § 212(e)(7), 116 Stat. at 651 (codified at 42 U.S.C.A. § 8401).

190. *Id.* § 201(a), 116 Stat. at 641 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e)(7) to the Public Health Service Act); § 212(e)(7), 116 Stat. at 651 (codified at 42 U.S.C.A. § 8401).

191. *Id.* § 201(a), 116 Stat. at 641 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e)(7) to the Public Health Service Act); § 212(e), 116 Stat. at 651 (codified at 42 U.S.C.A. § 8401).

192. *Id.* § 201(a), 116 Stat. at 639 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(e)(1) to the Public Health Service Act); § 212(e)(1), 116 Stat. at 649 (codified at 42 U.S.C.A. § 8401).

193. *See* 42 C.F.R. § 73.11 (2003); 9 C.F.R. § 121.12 (2004); 7 C.F.R. § 331.11 (2004). The CDC's regulations are more specific than APHIS', although the general focus of both is the same. In interpreting both sets of regulations to harmonize them, particularly for overlap agents and toxins, the more specific and stringent requirements of each set will likely govern.

194. 42 C.F.R. § 73.11; 9 C.F.R. § 121.12; 7 C.F.R. § 331.11. *See* CDC, Laboratory Security and Emergency Response Guidance for Laboratories Working with Select Agents, *at*

separate areas where listed, non-exempt agents or toxins are stored or used from "public areas of buildings," meaning areas that are not secured in accordance with the security plan developed under the regulations.[195] Academic institutions are accustomed to securing refrigerators and other containers for dangerous materials. Consistent with the open and collaborative research culture of academic institutions, however, such institutions are less accustomed to prohibiting sharing of research and storage areas among researchers and to requiring such areas to be isolated and separated, except in extraordinarily unusual circumstances involving the most dangerous materials. The physical separation and security measures required for all BPARA-regulated agent and toxin security plans challenge the collaborative research culture that is common in academic settings to foster innovation. Investigators who are not working with regulated agents or toxins and are not approved through the security risk assessment process cannot share work or storage areas, even temporarily, with those who are using such materials.[196] An investigator who is cleared for particular agents, toxins, and areas cannot share work or storage areas with an investigator who is cleared for other agents, toxins, or areas, unless they both pursue registration for all such materials and areas.[197] Significant and costly physical renovations and security system investments may be necessary to separate agent and toxin areas from other areas of a building, depending on building layout and security prior to adoption of the BPARA's regulations.

For areas, the security plan must include:[198] (a) inventory controls that satisfy the regulations' record-keeping requirements; (b) requirements for individuals who have access to agents or toxins to have at least an articulated minimum level of relevant education and experience; (c) physical and cyber security; (d) procedures for routine cleaning and maintenance activities; (e) measures to ensure that unescorted access to agent or toxin areas is available only by individuals who are approved through the security risk assessment process and, even then, only during hours necessary to perform a specific job and for a specifically authorized function; (f) measures to allow access to such areas by individuals who do not seek security risk assessment approval only if they legitimately need access for cleaning or other non-laboratory functions and are escorted and continually monitored by an individual who is approved through the security risk assessment process; (g) a program for security training for all individuals who have access to agent or toxin areas or containers, including laboratory personnel who work with the agents and

http://www.cdc.gov/mmwr/pdf/rr/rr5119.pdf (last visited Apr. 4, 2004) [hereinafter CDC Guidance for Laboratories].

195. 42 C.F.R. § 73.11(e). *See* CDC Guidance for Laboratories, *supra* note 194.

196. *See* 9 C.F.R. § 121.12(a)(2)(iv)(F); 42 C.F.R. § 73.11(d)(6); 7 C.F.R. § 331.11(a)(2)(iv)(F).

197. *See supra* Part III.A.4.a and *supra* notes 114, 177–78 and accompanying text. The application for registration and approval of access to agents and toxins requires each individual to list those agents or toxins to which he or she will have access and any changes must be reported to the Secretary of HHS or USDA as applicable. Access approval is for those agents or toxins listed in the application.

198. *See* 7 C.F.R. § 331.11; 9 C.F.R. § 121.12; 42 C.F.R. § 73.11; CDC Guidance for Laboratories, *supra* note 194. *See also infra* Part III.A.6.

toxins on a regular basis and, consequently, are approved through the security risk assessment process, as well as non-laboratory personnel and visitors, who are escorted in agent and toxin areas at all times by a person who is approved through the security risk assessment process; (h) card, keypad, and other access security measures that provide a unique access code for each individual who is approved to have access to agents and toxins; protocols to change such codes upon staff changes or loss or compromise of keys or passwords; prohibition against sharing such codes among individuals; and protocols requiring an individual to immediately report a loss or compromise of such code, keys, passwords, etc., to the entity's Responsible Official; (i) protocols for requiring an individual to immediately report to the entity's Responsible Official (1) suspicious or unauthorized people (and for removing such people) and (2) any loss, theft, or releases of agents or toxins or any sign of alteration or compromise of inventory records; (j) inspection of all packages on entry and exit from an agent or toxin area;[199] and (k) intra-entity agent and toxin transfer protocols, including the requirement that a person approved in the security risk assessment process must supervise packaging and moving agents and toxins. For agent and toxin container security, the security plan must specify the security measures, including locking such containers, providing a unique access code to each person who is approved through the security risk assessment process to have access, and prohibiting an individual from sharing such code, and, "as needed," providing for video surveillance of agent and toxin containers when they are not in direct view of an approved individual.[200] The Responsible Official must review the security plan annually and after each incident.[201]

An entity may implement alternatives to some of the security plan requirements for agent and toxin areas and containers, as long as such alternatives provide equivalent or greater security.[202] An early CDC guidance on the regulations states that "the regulations do recognize that access to a select agent or toxin can, as a practical matter, be limited by either security containers or by escorts."[203] It is unclear when the CDC or APHIS is requiring escorts and when they are finding

199. According to the CDC's answers to frequently asked questions, "packages" means "a wrapped or boxed object, parcel or container in which something is packed." CDC FAQ, *supra* note 23. This definition does not appear to include backpacks or hand bags, although the answer is unclear on this point and the CDC offers that its answer describes a minimum standard and that greater measures may be necessary depending on the circumstances. *Id*. An institution is well-advised to be explicit in its security plan on how the institution will define "packages," to tie this definition to the risk of the agents and toxins involved, and to advise the CDC or APHIS, as applicable, on how the institution will define and handle packages to provide the agency with an opportunity to object and to provide the institution with some defense if the agency later does not agree with the institution's plan.

200. *See* 7 C.F.R. § 331.11; 9 C.F.R. § 121.12; 42 C.F.R. § 73.11; CDC Guidance for Laboratories*, supra* note 194

201. *See* 42 C.F.R. § 73.11(c)); 9 C.F.R. § 121.12(b); 7 C.F.R. § 331.11(b).

202. *See* 42 C.F.R. § 73.11(d) (alternatives to the security measures summarized and listed as measures § 73.11(e), (f), (h) (respecting non-sharing of required unique individual access codes), § 73.11(i)–(k) in Part III.A.5, *supra*, may be implemented if the alternatives provide as great or greater security).

203. CDC FAQ, *supra* note 23.

secured containers to be adequate to satisfy the security of agent and toxin *areas* requirement and the prohibition against an entity allowing access to listed, non-exempt agents and toxins to anyone who is not approved through the security risk assessment process. The CDC's and APHIS' requirements may vary in relation to the risk posed by the agents and toxins that are involved. In any event, the institution should always keep in mind the law enforcement and anti-terrorism orientation of this law. An institution should be explicit during the registration process as to how the institution is interpreting the access restrictions and regulatory security requirements, and why any alternative to the measures specified in the regulations is both equivalent to the regulatory measures and appropriate for the level of risk the relevant agents and/or toxins pose.[204]

6. Record-keeping

The regulatory record-keeping requirements are closely related to the regulatory security requirements. An entity and Responsible Official must keep up-to-date, accurate and verifiable records for three years of: (i) all individuals who receive a security risk assessment approval;[205] (ii) an inventory of agents and toxins including names; characteristics, sources, acquisition dates, and quantities acquired of each agent and toxin;[206] quantities of each toxin (but not agent) on the date of the first inventory as well as held currently;[207] quantity, volume, mass, and date when each agent and toxin is destroyed[208] (see also the requirement for five business day advance notice to the relevant Secretary prior to destruction to discontinue use[209]); quantity and dates of any toxin's use;[210] date, parties, and quantities of agents or toxins transferred (including within the entity, even if all parties are covered by the same registration);[211] agents or toxins lost, stolen, or unaccounted for with a written explanation of discrepancies;[212] (iii) the name of each individual who accesses an agent or toxin, the identification of the agent or toxin accessed, the dates when agents or toxins are removed and returned if from or to long-term storage or stock culture holdings, and the quantity of any toxin (but not agent) removed or returned;[213] (iv) the name of, and date and time when, each individual enters or leaves an area where agents or toxins are used or stored, and if the individual is not approved through the security risk assessment process, the

204. *See id*. ("'Access' as it is used in these regulations takes on its ordinary meaning: 'the freedom or ability to obtain and make use of.' Anyone, including visitors, who have the freedom or ability to obtain and make use of a select agent or toxin, must be approved. . . . However, the regulations do recognize that access to a select agent or toxin can, as a practical matter, be limited by either security containers or by escorts.").

205. 42 C.F.R. § 73.15; 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

206. 42 C.F.R. § 73.15; 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

207. 42 C.F.R. § 73.15. *See* 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

208. 42 C.F.R. § 73.15. *See* 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

209. 42 C.F.R. § 73.7; 9 C.F.R. § 121.7; 7 C.F.R. § 331.6.

210. 42 C.F.R. § 73.15. *See* 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

211. *Id. See* 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

212. *Id. See* 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

213. *Id. See* 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

approved individual who accompanied such other individual at all times;[214] (v) safety inspections;[215] (vi) safety, security, and emergency response plans and incident reports;[216] (vii) training records;[217] and (viii) agent and toxin transfer documents and permits.[218]

7. Safety Plan

Entities must develop and implement a safety plan to protect researchers and others from injuries caused by listed, non-exempt agents and toxins. The plan should reflect the standards for level 2, 3, or 4 biological laboratories (commonly referred to as BL 2, 3, or 4 laboratories) that are applicable to the agents and toxins involved, as provided in the CDC's and National Institutes of Health's ("NIH") guidelines, "Biosafety in Microbiological and Biomedical Laboratories" ("BMBL")[219] and its appendices (other than Appendix F[220]) for HHS and overlap agents,[221] the NIH "Guidelines for Research Involving Recombinant DNA Molecules"[222] for genetic elements and recombinant nucleic acids and organisms, and the OSHA laboratory standard and requirements for hazard communications[223] and the BMBL, Appendix I, for toxins.[224] For APHIS agents and toxins, the plan should reflect the standards in BMBL, Appendix F.[225] An entity's Responsible Official must conduct inspections regularly, at least annually, to ensure proper implementation of the safety plan, and must document any deficiencies found and their correction.[226]

The HHS or Agriculture Secretary, as appropriate, must approve any experiments with recombinant DNA that deliberately transfer a drug resistant, non-naturally occurring, trait to HHS, USDA, or overlap agents that could "compromise the use of the drug to control disease agents in humans, veterinary medicine, or agriculture" before the experiments are undertaken.[227] Similarly, the Secretary must pre-approve any activity that deliberately forms recombinant DNA

214. *Id. See* 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

215. 42 C.F.R. § 73.15; 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

216. 42 C.F.R. § 73.15; 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

217. 42 C.F.R. § 73.15; 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

218. 42 C.F.R. § 73.15; 7 C.F.R. § 331.14; 9 C.F.R. § 121.15.

219. CDC, Health and Safety Topics, *available at* http://www.cdc.gov/od/ohs/pdffiles/4th%20BMBL (on file with the author) [hereinafter CDC BMBL].

220. *Id*.

221. *Id.;* 42 C.F.R. § 73.10.

222. NIH, Guidelines for Research Involving Recombinant DNA Molecules, *at* http://www4.od.nih.gov/oba/rac/guidelines/guidelines.html (last visited Apr. 4, 2004) [hereinafter NIH Guidelines].

223. 29 C.F.R. §§ 1910.1450, 1910.1200 (2003).

224. NIH Guidelines, *supra* note 222.

225. *See* CDC BMBL app. F, *supra* note 219. *See* 9 C.F.R. § 121.12 (2004); 7 C.F.R. § 331.11 (2004); CDC, Morbidity and Mortality Weekly Report*, at* http://www.cdc.gov/mmwr (last visited Apr. 4, 2004).

226. *See* CDC FAQ, supra note 23; CDC Guidance for Laboratories, *supra* note 194; 42 C.F.R. § 73.10 (2003).

227. 42 C.F.R. § 73.10; 9 C.F.R. § 121.10 (2004).

genes for "biosynthesis of select toxins" and/or that have a Lethal Dose 50 for vertebrates of less than 100 nanograms per kilogram body weight.[228]

8. Transferring or Acquiring Agents or Toxins

An entity or other person is prohibited from transferring any listed, non-exempt agent or toxin to another entity or other person in the United States, or from receiving any such agents or toxins from any entity or person outside the United States, unless (i) the sender and the U.S. recipient fulfill the CDC's or APHIS' requirements, as applicable, for securing agency pre-transfer approval and for filing transfer documentation with the agency, and are registered under the regulations for the agent or toxin being transferred, (ii) the sender from outside the United States satisfies all import requirements, (iii) all senders satisfy applicable packaging and shipping laws, (iv) the Responsible Official for the recipient sends the required transfer documentation to the sender and HHS or USDA Secretary (through CDC or APHIS) within two business days of receipt of such agent or toxin, (v) the Responsible Official for the recipient "immediately" reports to the Secretary (through CDC or APHIS) if the agent or toxin is not received within forty-eight hours of its expected delivery or if their packaging is leaking or damaged, and (vi) the Responsible Official for the transferor also ensures that listed, non-exempt agents and toxins are only transferred to recipients who are registered and in compliance with the transfer requirements of the BPARA regulations.[229] These requirements do not apply to intra-entity transfers if the sender and the recipient are under the same registration certificate, but do apply if the sender and the recipient are not under the same registration certificate.[230] If an entity has more than one location, it will have a separate registration certificate for each location and, consequently, will have to comply with transfer requirements when transferring agents or toxins from one of its locations to any other.[231]

9. Requirements for Notifications

Any entity that must register under the regulations must comply with the regulatory notice requirements for thefts, losses, or releases of listed, non-exempt

228. 42 C.F.R. § 73.10(c); 9 C.F.R. § 121.10(c).

229. 42 C.F.R. §§ 73.9(c)(4), 73.14; 9 C.F.R. §§ 121.10(a)(4), 121.14; 7 C.F.R. §§ 331.9(a)(4), 331.13 (2004).

230. *See* 42 C.F.R. §§ 73.9(c)(4), 73.14; 9 C.F.R. §§ 121.10(a)(4), 121.14; 7 C.F.R. §§ 331.9(a)(4), 331.13 (there are minor differences in CDC's and APHIS' regulations, although the general focus of both is the same; in interpreting the regulations to harmonize them, particularly for overlap agents and toxins, the stricter and more specific of both sets will likely govern). Agency approval for overlap agents or toxins may be given by CDC or APHIS. Note that export control laws and regulations govern transfers abroad of certain agents, toxins and other chemicals. *See infra* Part VI.

231. *See* 42 C.F.R. §§ 73.9(c)(4), 73.14; 9 C.F.R. §§ 121.10(a)(4), 121.14; 7 C.F.R. §§ 331.9(a)(4), 331.13 (the regulations provide that the transfer requirements do not apply to intra-entity transfers if the same registration certificate applies; consequently, if there are two locations and two certificates, the transfer requirements do apply); *supra* notes 168–69 and accompanying text.

agents or toxins. Immediate notice to the Secretary of HHS or Agriculture (through CDC or APHIS) and to state and local law enforcement is required by telephone, e-mail, or telecopier for HHS agents or toxins,[232] and to Federal, state, and local law enforcement by telephone for USDA and overlap agents or toxins, upon the discovery of the loss or theft of any such agent or toxin.[233] The CDC requires notification even if the responsible parties are identified and even if the material is recovered.[234] The CDC specifies that the notice must include the name, characteristics, and estimated lost or stolen quantity of the agent or toxin, and the estimated time and location of the loss or theft.[235] Immediate notice to the Secretary and state and local public health agencies is required through the same means, upon any release of a listed, non-exempt agent or toxin that causes occupational exposure or is outside of the applicable primary containment barriers.[236] The CDC requires that this notice must include the name, characteristics, hazards posed, and the estimated quantity of the agent or toxin so released, estimated time and duration of the release, a description of the environment (including buildings and man-made structures as well as the natural environment) into which, and the location from which, the release occurred, the number of people potentially exposed at the "facility," and any response actions taken.[237] Within seven calendar days of any such loss, theft, or release, the entity must provide a written report to the Secretary through the CDC or APHIS on the appropriate agency form.[238] CDC and APHIS makes the Responsible Official (or Alternate Responsible Official) responsible for giving these notices.[239] Individuals with access to agent or toxin areas are required under the security plan to immediately notify the Responsible Official when there is a theft, loss, or release as discussed in Part III.A.5 of this article.

The Secretaries of HHS and Agriculture must notify Congress of the number and nature of thefts, losses, and releases of listed, non-exempt agents and toxins annually.[240] The Act also requires the Secretary of HHS to confer with other federal agencies and then to report to Congress within one year after enactment of

232. 42 C.F.R. § 73.17(a).

233. 9 C.F.R. § 121.17(a); 7 C.F.R. § 331.16.

234. 42 C.F.R. § 73.17(b).

235. 42 C.F.R. § 73.17(c)(1)–(4).

236. 42 C.F.R. § 73.17(d); 9 C.F.R. § 121.17(b); 7 C.F.R. § 331.16(b).

237. 42 C.F.R. § 73.17(e)(1)–(8).

238. 42 C.F.R. § 73.17(f); 9 C.F.R. § 121.17(c); 7 C.F.R. § 331.16(c). *See also* BPARA § 201(a), 116 Stat. 594, 645 (codified at 42 U.S.C.A. § 262a (2003)) (adding Section 351A(j) to the Public Health Service Act) (requiring the entity to notify CDC and local and state authorities in connection with HHS agents or toxins); § 212(j), 116 Stat. at 656 (codified at 7 U.S.C.A. § 8401 (West Supp. 2003)) (requiring the entity to notify APHIS and local and state authorities in connection with USDA agents or toxins). Entities should notify CDC or APHIS and local or state authorities in connection with overlap agents. *See* 42 C.F.R. § 73.21 for specific requirements relating to forms, notices, and submission.

239. 42 C.F.R. § 73.9(c)(5); 9 C.F.R. § 121.17(a); 7 C.F.R. § 331.16(a).

240. BPARA § 201(a), 116 Stat. at 645 (codified at 42 U.S.C.A. § 262a) (adding Section 351A(k) to the Public Health Service Act); § 212(k), 116 Stat. at 656 (codified at 7 U.S.C.A. § 8401).

the BPARA on the extent to which government and private entities are complying with the regulations and evaluating the impact of the regulations on research, among other topics.[241]

10. Emergency Preparedness and Response

The regulations require that an entity develop and implement an emergency response plan, and the CDC requires the plan to generally meet OSHA's hazardous waste and emergency response standards.[242] The plan must address bomb threats, natural disasters such as earthquakes and severe weather, and power failures, and must coordinate with entity-wide and outside parties' emergency preparedness and response plans.[243] It must address agent and toxin hazards, the roles of emergency responders, training requirements, emergency communications, measures to prevent the occurrence of emergencies, information about safe distances, measures for controlling emergency sites, and measures for security, evacuation, taking refuge, and decontamination.[244] The plan must include information about medical resources and treatment and provide for personal protective equipment.[245] The plan must include procedures for post-incident review, critique, and corrective actions.[246]

11. Training Requirements

An entity must develop and implement a training program on its safety, emergency response, and security plans and the related regulatory requirements for listed and non-exempt agents and toxins.[247] Training in these matters is required before work in an agent or toxin area begins (whether or not the person will be working with these materials) and before any new exposures to agents or toxins occur.[248] Annual refresher training is required, for (i) all individuals with access to such agents or toxins who require approval through the security risk assessment process; and (ii) all individuals who are visitors or otherwise have escorted access to areas where such agents or toxins are used or stored (e.g., custodial staff, non-laboratory workers, and visitors).[249] The Responsible Official must provide the training and the training must include a means of verifying that the person being

241. *Id.* § 201(b), 116 Stat. at 646 (not codified, but published as 42 U.S.C.A. § 262a note). At the time this article went to the printer, these reports had not yet been published.

242. 29 C.F.R. § 1910.120 (2003). *See also* CDC Guidance for Laboratories, *supra* note 194. The CDC's regulations are more specific than APHIS's, but the scope and focus of both are the same. In interpreting the two sets of regulations to be harmonious, particularly for overlap agents and toxins, the more specific and stringent requirements of each set will likely govern.

243. 42 C.F.R. § 73.12(b)–(c). *See also* 9 C.F.R. § 121.12(a)(3), 7 C.F.R. § 331.11(a)(3).

244. 42 C.F.R. § 73.12(b)–(c). *See also* 9 C.F.R. § 121.12(a)(3), 7 C.F.R. § 331.11(a)(3).

245. 42 C.F.R. § 73.12(b)–(c). *See also* 9 C.F.R. § 121.12(a)(3), 7 C.F.R. § 331.11(a)(3).

246. 42 C.F.R. § 73.12. *See also* 9 C.F.R. § 121.12(a)(3), 7 C.F.R. § 331.11(a)(3).

247. 42 C.F.R. § 73.13(a); 9 C.F.R. § 121.13(a); 7 C.F.R. § 331.12(a).

248. 42 C.F.R. § 73.13(b); 9 C.F.R. § 121.13(b); 7 C.F.R. § 331.12(b).

249. 42 C.F.R. § 73.13(b); 9 C.F.R. § 121.13(b); 7 C.F.R. § 331.12(b).

trained understands the training.[250] A Responsible Official who determines that certain individuals have experience "handling" listed, non-exempt HHS agents or toxins, may "certify in writing that the individual has the required knowledge, skills, and abilities to safely carry out the duties and responsibilities" covered in the training, in lieu of the initial training.[251] Such individuals must take annual refresher training.[252]

Note that if listed, non-exempt agents or toxins are used in training, the individuals who have access must have been approved through the security risk assessment process.[253] In addition, information must be provided to the CDC (and presumably to APHIS if applicable) at least eight weeks before the training on who will have access to the regulated agents or toxins (through an updated table 4B of the entity's registration application), the date of the training, the room and building location of the training, and the purpose of the training.[254]

B. How to Approach a Compliance and Implementation Program Under the USA PATRIOT Act Bioterrorism Provisions and the BPARA

1. Knowing the Scope of an Institution's Regulated Community

The foundations of any program to support compliance with and implementation of the bioterrorism provisions of the USA PATRIOT Act and the BPARA are (a) central institutional knowledge of which research groups are using biological materials generally (and, consequently, are subject to Section 817(1) of the USA PATRIOT Act), and of the smaller number of research groups that are using listed agents or toxins (and, consequently, may be subject to the BPARA and Section 817(2) of the USA PATRIOT Act as well), and (b) knowledge by each member of these groups, and by the staff who support their work, about the requirements and prohibitions of these federal laws.

An effective approach to gaining the necessary knowledge and disseminating the necessary information initially is for the institution's Environment, Health and Safety ("EHS") Office and a senior officer who is responsible for research (such as the provost or vice president of research) to jointly notify all principal investigators ("PI") who may be working with *any* biological materials about the existence and basic prohibitions and requirements of Sections 817(1) and 817(2) of the USA PATRIOT Act and of the existence of the BPARA and its regulations. The

250. 42 C.F.R. § 73.13(e). *See also* 9 C.F.R. § 121.13; 7 C.F.R. § 331.12. The CDC's regulations are more specific than are APHIS', but all require this scope of training initially and annually. In trying to harmonize the two sets of regulations, particularly for overlap agents and toxins, the more specific and stringent is likely to govern. Some institutions include a required quiz as part of their training program to determine whether the participants successfully completed and understood the training. Records of the quiz and quiz results should be maintained to demonstrate that the institution satisfied the training program requirements.

251. 42 C.F.R. § 73.13(d).

252. 42 C.F.R. § 73.13(b), (d).

253. *See* CDC FAQ, *supra* note 23.

254. *Id.*

institution's counsel's office, or if none, outside counsel, should assist in the preparation of this summary, and it is important to state clearly that the summary is not all-inclusive and to provide easy access to more detailed information as well as a contact who can answer questions and provide guidance. Note that this population is often broader than the members of the institution's biology department, and may include members of the chemistry department, certain engineering departments, medical schools or departments, among others. The institution's Office of Sponsored Programs or other office that administers research funding, is also a good source of information on who may be undertaking biological research ("OSP").

If this approach is taken, as part of the general notice or in a separate document, the EHS office should issue a survey to all of the PIs whose research groups may use biological materials of any kind to determine which groups use agents or toxins that are listed under the BPARA's regulations, and of those, which fall under an exclusion or exemption from the regulatory requirements. The survey or other outreach should also elicit information on the identity of individuals in the PI's research group or supporting the group's work. Appendix E[255] includes an example of such a survey document. The EHS office should track the issuance and responses to the survey and follow up as necessary to obtain complete responses. If particular responses do not seem correct based on the general knowledge of the EHS office, the office should follow up to corroborate the responses. The EHS office should also follow up to confirm that any claimed exemption or exclusion is correct under the BPARA and its regulations in order to assist the school's regulated community in not inadvertently violating the regulations. From the survey responses and any follow up, the EHS office can identify which research groups use listed agents or toxins, and can then categorize them as covered by the detailed provisions of the BPARA and its regulations, as well as Sections 817(1) and 817(2) of the PATRIOT Act, or as covered by only the more general prohibitions of Section 817(1) of the PATRIOT Act relating to the types and quantities of biological materials obtained, possessed and retained. These records should also note whether the limited USA PATRIOT Act coverage is based on a confirmed exclusion or exemption from the BPARA's regulations or on the fact that no BPARA-listed agents or toxins are involved. This information should be kept confidential to the greatest extent possible to support security requirements of the BPARA's regulations.

Institutions may consider issuing similar surveys periodically. In any event, it is a good idea for the EHS office and OSP to develop a screening process under which OSP may assist the EHS office in continuously identifying any proposed research that may involve biological materials generally, or agents or toxins listed under the BPARA's regulations specifically. Researchers generally must apply for funding to support new activities through OSP, and capturing information about activities involving biological materials before they begin will assist in keeping the

255. For Appendix E, Important Federal Law Compliance Survey Re: Biological Agents/Toxins, visit The Journal of College and University Law, Symposium Webpage, *at* http://www.nd.edu/~jcul/USA_PATRIOT_Act/Appendix_E.pdf (last visited Apr. 4, 2004).

EHS office's records up to date, minimize the frequency of surveys, and assist researchers and their staffs to comply with laws that are enforced with extreme seriousness. Appendix F[256] contains an example of such screening provisions of an OSP proposal application form.

2. Helping Individuals to Comply

The EHS office, and possibly one of the institution's lawyers, should have an initial meeting with the PIs whose research groups are determined to use listed, non-exempt agents or toxins that are governed by the BPARA, and should provide these PIs with a USA PATRIOT Act self-assessment questionnaire and more detailed information about Section 817(2) of the USA PATRIOT Act and the BPARA. The same approach should be taken with PIs who are later identified through the OSP screening process or surveys as initiating work with regulated agents and toxins. Even after the enactment of the BPARA and its allocation of background checking responsibility to the U.S. Attorney General, the USA PATRIOT Act imposes criminal penalties on individuals who are "restricted persons" and violate the USA PATRIOT Act's Section 817(2) prohibitions. Consequently, it is important for individuals to self-assess whether they are "restricted persons" before they possess, transport, ship, or receive listed non-exempt agents or toxins. Appendix A[257] to this article contains examples of these questionnaires, all of which require some form of return certification to the EHS office or counsel's office.[258] The PIs should have a chance to ask questions and should be instructed to provide the questionnaire to all individuals in their research groups and to all of their administrators and other staff who support their work (e.g., those who order or arrange for shipping or receiving listed, non-exempt agents or toxins, and those who assist in storage or research activities). Again, the EHS office should track the return of these assessment questionnaires by all such PIs and all members of their research groups who use listed, non-exempt agents or toxins.

The EHS office, counsel's office, vice president of research and leaders of faculty in biological research areas may find it helpful to form an ad hoc task force for the implementation of these anti-bioterrorism laws. Such a task force can ensure that the EHS office devises approaches that will serve the academy well and will be sustainable in the academy, and that the EHS office has the necessary support to oversee implementation. With the support of such a task force, an institution might decide to purchase all listed toxins centrally through the EHS office so that this office may ensure that PIs whose toxins are excluded from the BPARA's regulations because they use volumes below the per PI toxin volume exclusions, remain below such volume thresholds, and do not inadvertently exceed the limits and become subject to, and violate, the detailed regulatory

256. For Appendix F, Investigator Certifications and Questions, Symposium Webpage, *at* http://www.nd.edu/~jcul/USA_PATRIOT_Act/Appendix_F.pdf (last visited Apr. 4, 2004).

257. *See* Appendix A, *supra* note 31.

258. See *supra* Part II for a description of the different approaches to these questionnaires.

requirements.[259] All listed, non-exempt agents must be purchased centrally through the institution's Responsible Official.[260]

3. Consents and Institutional Actions

With the enactment of the USA PATRIOT Act and the BPARA, an institution should take steps to identify the actions it seeks to take (and to ensure that the institution is able to take such actions), if an individual self-identifies or is determined by the institution or the U.S. Attorney General to be a "restricted person" under the USA PATRIOT Act,[261] or is otherwise unable to legally have access to listed non-exempt select agents and toxins, when the person's work or study at the institution requires such access. In connection with new employment and appointments, or renewals of contracts or appointments, the following sample language may be included in the employment offers and appointment letters:

> An essential condition and requirement of your initial and continued [appointment or employment] by [institution] is your ability to legally access, possess, and use all materials that may be involved in the work you are to perform, or to which you may be exposed, at [institution], under applicable laws and regulations in effect from time to time.

The institution should have a plan that takes into account its own policies and procedures as well as the state and federal employment, labor, and other laws and contracts to which it is subject, in connection with employees, students, and other personnel who are already at the institution.

In connection with undertaking the registration and security risk assessment application processes under the BPARA, an institution may want to ask any of its personnel who will need to participate in these processes to sign the institution's consent form (in addition to the required FBI consent form) allowing the institution to disclose information it has or receives about the individual.[262] A sample consent form that satisfies FERPA and likely satisfies most other consent requirements may state:

> I authorize [institution] to release to the United States Department of Health and Human Services, the United States Department of Agriculture, the United States Attorney General and Justice Department, the Federal Bureau of Investigation and any other governmental authority, and any agent or contractor of a governmental authority, any of my personal information, including individually identifiable information, that [institution] has or receives and that may be requested under any laws or regulations and related administrative practices, including but not limited to the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 and its regulations and the USA PATRIOT Act, that govern biological agents

259. *See supra* Part III.A.3, 4; and note 79 and accompanying text.

260. *See supra* Part III.A.8.

261. *See supra* Part II.B and note 30 and accompanying text.

262. *See supra* Part III.A.4.a and accompanying notes; *supra* note 35.

> or toxins. I understand that the purpose of such disclosure is to permit me, and/or [institution], to apply to the federal government for permission to possess and have access to such agents and toxins in connection with my study or work at [institution] or to otherwise comply with applicable laws. I further understand that information disclosed about me may include, for example, but is not limited to: my name, date of birth, fingerprints, home and school addresses, telephone numbers, e-mail addresses, and social security number. This consent supplements my consent in the FBI security risk assessment form, which also shall apply to [institution].

The security risk assessment process is alien, and possibly intimidating, to academic researchers. Consequently, an institution's counsel and Responsible Official may consider meeting with the individuals who need to sign the consent to ensure that they understand the scope and purpose and have an opportunity to ask questions.

If the FBI were to request medical or mental health records that the institution maintains concerning an individual, a separate "HIPAA-compliant" consent would be required from the individual.[263] Neither the general consent just quoted, nor the consent form included in Section V of the FBI's security risk assessment application form, references medical and mental health records, or satisfies the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[264] Institutions have developed their own HIPAA and similar state law compliance programs, and are well advised to maintain consistency in their implementation practices. Consequently, the institution should follow its HIPAA notice and consent practices in responding to any requests for medical or mental health records in the security risk assessment process.

When the institution transmits applications to CDC or APHIS and the FBI, it is important if any students are among the individuals covered by the applications, that the institution's transmittal letter notifies the agencies about the applicability and restrictions imposed by FERPA on the use and re-disclosure of the information provided.[265] To meet this requirement, the transmittal letter may state:

> Some of the information provided in the enclosed applications constitutes student "education records" that are subject to the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g and its regulations at 34 C.F.R. pt. 99.0 ("FERPA"). This information is being provided to the United States Department of Health and Human Services, the United States Department of Agriculture, the United States Attorney General and Justice Department, the Federal Bureau of Investigation and their respective employees, agents, and contractors in the select agent and toxin program, for purposes of implementing the Public Health Security and Bioterrorism Preparedness and Prevention

263. *See supra* Part III.A.4.a and accompanying notes; *supra* note 35.

264. *See supra* notes 35, 120, 152–61 and accompanying text; *supra* Part III.A.4.a, b.

265. *See id.*; *supra* Part III.A.4.a, b; 20 U.S.C.A. § 1232g(b)(2)(A), 4(B) (2000 & West Supp. 2003); 34 C.F.R. §§ 99.30(b), 99.32(b), 99.33(a), (b), (d) (2003).

> Act of 2002 and its regulations, pursuant to the authority contained in FERPA. Pursuant to FERPA, this information is being provided on the condition that the intended recipients may not use the information for any purpose other than the purposes for which the disclosure of this information is being made, and on the condition that such recipients will not disclose this information to any other person, without the prior written consent of the affected student.

IV. USA PATRIOT ACT AMENDMENT OF FERPA[266]

The USA PATRIOT Act supports increased anti-terrorism activities by federal law enforcement agencies by enhancing their authority to conduct investigations, as well as by easing the related procedural and other conditions to securing or exercising such authority. These changes affect many institutions and their members, including academic institutions. Some, including members of Congress and other leaders in the federal government, have expressed the view that colleges and universities are potential training and hiding venues for terrorists.[267] It is not clear why colleges and universities have been singled out for this concern, as foreign terrorists may learn valuable lessons in any number of venues in the United States and around the world. Also, as MIT President Charles M. Vest noted in his address to the 2002 annual meeting of the National Association of College and University Attorneys, the terrorism of September 11 did not involve advanced science or require a college or university education.[268] Nevertheless, most colleges and universities will be visited by federal law enforcement or receive a subpoena, court order or search warrant in a federal criminal or anti-terrorism investigation at some time; many have already. It is important for colleges and universities to be prepared to respond appropriately. Knowing the applicable laws and ensuring that the institution's policies establish the environment sought by the institution while also being consistent with legal requirements, are critical.

Whenever a college or university receives a subpoena, court order, or search warrant for information or records involving a student, FERPA is likely to apply. Section 507 of the USA PATRIOT Act amends FERPA by adding a new subsection (j)[269] to permit certain disclosures of individually identifiable records of a student that are maintained by a college or university (defined as "education records"[270]) funded by the U.S. Department of Education, without the prior written consent of the student, notwithstanding FERPA's general prohibition against such

266. USA PATRIOT Act, § 507, 115 Stat. 272, 367–68 (codified at 20 U.S.C.A. § 1232g(j) (2000 & West Supp. 2003)).

267. *See, e.g.,* Knezo, *supra* note 4, at 4–17, notes 7, 15, 27, 35, 54. A higher education, however, may not be needed for the kind of terrorism against the United States that we have seen to date. *See, e.g.,* Vest, *supra* note 4.

268. Charles M. Vest, Openness, Opportunity, and Security in Universities: A National Challenge, National Association of College and University Attorneys Annual Meeting, Boston, Mass. (June 26, 2002), *available at* http://www.web.mit.edu/president/communications/nacua.html.

269. USA PATRIOT Act § 507, 115 Stat. at 367–68 (codified at 20 U.S.C.A. § 1232g(j)).

270. 20 U.S.C.A. § 1232g(a)(4)(A)–(B) (2000).

disclosures.[271] The new subsection permits the U.S. Attorney General, or any federal officer or employee in a position of Assistant Attorney General or higher who is designated by the Attorney General, to submit a "written application to a court of competent jurisdiction for an ex parte order" requiring the college or university to allow the Attorney General or his designee to "collect . . . retain, disseminate, and use" education records in connection with the investigation or prosecution of certain crimes relating to domestic or international terrorism.[272]

271. *Id.* § 1232g(b)(1)–(2) (2000). FERPA permits colleges or universities to make "directory information" publicly available without the prior written consent of the student, provided that the institution gives "public notice of the categories of information which it has designated as [directory] . . . and . . . allow[s] a reasonable period of time after such notice . . . for [a student] . . . to inform the institution . . . that any or all of the information designated should not be released without the [student's] . . . prior consent." *Id.* § 1232g(a)(5)(B) (2000). Colleges or universities may include the student's name, address, telephone number, birth date and place, major field of study, officially recognized activities and sports, weight and height if the student is an athletic team member, dates of attendance, degrees and awards, and most recent previously attended educational institution, as well as any other information that "would not generally be considered harmful or an invasion of privacy," 34 C.F.R. § 99.3, in the college's or university's definition of directory information. *Id*. § 1232g(a)(5)(A) (2000). The college or university, however, is permitted to decide not to include all such information in its definition of "directory information" and some colleges or universities use more restrictive definitions in implementing FERPA and in their internal privacy policies. *Id.* § 1232g(a)(5)(A) (2000) (defining directory information), (B) (permitting release of directory information after notice), (d) (college students are to exercise the consent rights given parents of other students under FERPA); 34 C.F.R. § 99.3 (defining directory information to include the statutory list as well as additional information that is not considered harmful or an invasion of privacy), § 99.37 (establishing the conditions that apply to disclosing directory information). FERPA also provides certain exceptions to its general prohibition against disclosure of education records without the prior written consent of the student. *See* 20 U.S.C.A. § 1232g(b) (2000) (exceptions), § 1232g(h) (2000) (permitting disclosure of disciplinary records to teachers or college or university officials of other colleges or universities), § 1232g(i) (2000) (permitting disclosure to a parent or guardian of a student's violation of any law or of college or university policy governing alcohol or drugs, provided the student is under twenty-one and the college or university determines the student "committed a [related] disciplinary violation," unless state law prohibits such disclosure); 34 C.F.R. §§ 99.30–99.39. FERPA also permits disclosure of non-directory education records with the college or university student's written and dated consent, which must "specify the records that may be disclosed . . . the purpose [for] disclosure [and] the party or class . . . to whom disclosure may be made." The college or university must also condition its disclosure on the third party not disclosing the information to any other person and not using the disclosed information for any other purpose. *See* 20 U.S.C.A. § 1232g(b)(2)(A), (b)(4)(B), (d) (2000); 34 C.F.R. §§ 99.3, 99.5, 99.30(a)–(b), 99.33.

272. USA PATRIOT Act § 507, 115 Stat. at 367–68 (adding subsections (j)(1)(A) and (B) to FERPA); U.S. Department of Education, Recent Amendments to Family Educational Rights and Privacy Act Relating to Anti-Terrorism Activities, Dear Colleague Letter 2 & note 1 (Apr. 12, 2002), *available at* http://www.ifap.ed.gov/eannouncements/attachments/0412FERPA.pdf [hereinafter Dear Colleague Letter]. The federal crimes to which these orders must relate are listed in 18 U.S.C.A. § 2332b(g)(5)(B) (2000 & West Supp. 2003) (e.g., destruction of aircraft or aircraft facilities; violence at international airports; arson within special maritime and territorial jurisdiction; biological weapons; congressional, cabinet, and Supreme Court assassination and kidnapping; nuclear materials; plastic explosives; arson and bombing of Government property risking or causing death; arson and bombing of property used in interstate commerce; killing or attempted killing during an attack on a federal facility with a dangerous

Under the USA PATRIOT Act's amendment of FERPA, colleges and universities are not liable for producing such student records in response to the *ex parte* order of a court having jurisdiction, and are not required to keep records on the production.[273]

The federal crimes to which the education records that are subject to a FERPA subsection (j) court order must relate, include crimes of terrorism "calculated to influence the conduct of government," such as "destruction of aircraft, assassination, arson, hostage taking, destruction of communications lines or national defense premises, and use of weapons of mass destruction."[274] The Justice Department's application to the court must "certify that there are specific and articulable facts giving reason to believe" the records are relevant for such purpose.[275] The court must rely on such Justice Department certification and "shall issue" the order if the application contains this certification without making

weapon; conspiracy to murder, kidnap, or maim persons abroad; killing or attempted killing of officers and employees of the United States; murder or manslaughter of foreign officials, official guests, or internationally protected persons; hostage taking; destruction of communication lines, stations, or systems; injury to buildings or property within special maritime and territorial jurisdiction of the United States; destruction of an energy facility; Presidential and Presidential staff assassination and kidnapping; wrecking trains; terrorist attacks and other acts of violence against mass transportation systems; destruction of national defense materials, premises, or utilities; violence against maritime fixed platforms; certain homicides and other violence against U.S. nationals occurring outside of the United States; use of weapons of mass destruction; acts of terrorism transcending national boundaries; bombing of public places and facilities; harboring terrorists; providing material support to terrorists; providing material support to terrorist organizations; financing of terrorism; or torture) or an act of domestic or international terrorism as defined in 18 U.S.C.A. § 2331 (2000 & West Supp. 2003) ("international terrorism" means "activities that . . . involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; . . . appear to be intended . . . to intimidate or coerce a civilian population; . . . to influence the policy of a government by intimidation or coercion; or . . . to affect the conduct of a government by mass destruction, assassination or kidnapping; and . . . occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimate or coerce, or the locale in which their perpetrators operate or seek asylum;" and "domestic terrorism" means similar activities that "occur primarily within the territorial jurisdiction of the United States").

273. USA PATRIOT Act § 507, 115 Stat. at 367–68 (codified at 20 U.S.C.A. § 1232g(j)) (adding to FERPA subsections (j)(1) (providing for court orders for student education records in connection with the investigation or prosecution of certain terrorism and other crimes), (j)(2) (Justice Department application for order), (j)(3) (non-liability for good faith production), and (j)(4) (otherwise applicable record-keeping does not apply)); Dear Colleague Letter, *supra* note 272. The education records that are subject to a subsection (j) court order must be "relevant to an authorized investigation or prosecution . . . [under] section 2332b(g)(5)(B) of Title 18 [of the U.S.C.], or an act of domestic or international terrorism as defined in section 2331 of that title." 20 U.S.C.A. § 1232g(j)(1)(A) (2000 & West Supp. 2003).

274. *See* Dear Colleague Letter, *supra* note 272; USA PATRIOT Act § 507, 115 Stat. at 367–68 (codified at 20 U.S.C.A. § 1232g(j)) (adding subsections (j)(1)(A)–(B) to 20 U.S.C. § 1232g).

275. USA PATRIOT Act § 507, 115 Stat. at 367–68 (codified at 20 U.S.C.A. § 1232g(j)(2)(A)–(B)).

the court's own findings of fact on relevance.[276]

Whether the issuing court has jurisdiction to issue the order depends on the nature of the investigation. As the next Part of this article addresses, the USA PATRIOT Act expands the jurisdiction of federal courts to nation-wide jurisdiction in connection with some types of investigations, provided that the court has jurisdiction over the subject matter, i.e., the type of crime.[277] Consequently, a college or university may find that it receives a court order for education records from a federal court in another state or federal district and should not automatically conclude that the court lacks jurisdiction.

Although providing an exception to FERPA's general non-disclosure rule, the USA PATRIOT Act's amendment to FERPA creates a new subsection rather than an addition to the list of non-disclosure exceptions in existing subsection (b). Other exceptions are also provided in this manner.[278] This new non-disclosure exception that is created by the USA PATRIOT Act, however, concerns disclosures in response to certain court orders; and FERPA subsections (b)(1)(J) and (b)(2)(B) already establish two exceptions relating to court orders and to subpoenas. One existing exception applies to the production of education records in response to a federal grand jury subpoena or a subpoena "for a law enforcement purpose."[279] A college or university may produce records required under either of such subpoenas only after using reasonable efforts to first notify the student, unless the issuer orders the college or university not to inform the student.[280] The second existing exception applies to the production of education records in response to any judicial order or other "lawfully issued subpoena" following a reasonable effort to first notify the student.[281] The questions these existing provisions raise relate to whether the notice requirements that apply to grand jury and law enforcement subpoenas and judicial orders and other lawfully issued subpoenas under subsection (b)(1)(J) and (b)(2)(B) of FERPA also apply to a court order issued under the new subsection (j). Is a school required to give notice of a subsection (j) court order to a student before responding to a subsection (j) order under FERPA if the order is silent on giving notice? May a school voluntarily give such notice if a subsection (j) order does not prohibit notice, even if FERPA does not expressly require notice, or is a school prohibited to give notice to the student before responding to a subsection (j) order (and does the answer depend on whether the order prohibits notice or is silent)?

Section 507 of the USA PATRIOT Act provides for new subsection (j) court orders to compel production of education records without the consent of the

276. *Id.*

277. *Id.* § 220, 115 Stat. at 291–92 (codified at 18 U.S.C.A. §§ 2703, 2711 (2000 & West Supp. 2003)) (nationwide search warrants for electronic evidence); § 216(c), 115 Stat. at 288–90 (codified at 18 U.S.C.A. § 3127 (2000 & West Supp. 2003)) (defining a court of competent jurisdiction to authorize pen registers and trap and trace devices to be any federal district court or court of appeals with jurisdiction over the crime being investigated).

278. *See* 20 U.S.C.A. § 1232g(h)–(i) (2000).

279. *See id.* § 1232g(b)(1)(J) (2000 & West Supp. 2003).

280. *Id.*

281. *Id.* § 1232g(b)(2)(B) (2000); 34 C.F.R. § 99.31(a)(9) (2003).

student "[n]otwithstanding" subsections (a) through (i) of FERPA or any provisions of state law.[282] This could mean that subsection (b) of FERPA and state law do not apply at all, or that any provisions of subsection (b) or of state law that are inconsistent with new subsection (j) do not apply. The most likely interpretation of subsection (j)'s limitation on the application of FERPA subsection (b) and state law to FERPA subsection (j) court orders is that only those portions of subsection (b) and of state law that are inconsistent with subsection (j) do not apply, but that other portions do apply. This conclusion is based both on standard statutory construction of the word "notwithstanding" and on the composition of the rest of subsection (j).[283]

Section 507 of the USA PATRIOT Act expressly provides that a college or university need not keep records of disclosures made in response to a new subsection (j) court order, by providing that the requirement under FERPA subsection (b)(4)(A) (i.e., to keep records of most disclosures made under exceptions to the non-disclosure rule) does not apply to subsection (j) disclosures.[284] If the "notwithstanding" clause of subsection (j) covered every provision of subsection (b), there would be no need for this exclusion from the record-keeping requirement of subsection (b). By expressly excluding subsection (j) disclosures from the subsection (b)(4) record-keeping requirement, Congress evidences its determination that it was necessary to provide for such exclusion and implies that the record-keeping requirement would apply in the absence of the exclusion. Subsection (j), as added by Section 507 of the USA PATRIOT Act, does not expressly provide any relief from the subsection (b)(1)(J) or (b)(2)(B) requirement that the college or university use reasonable efforts to notify the student prior to making a disclosure of education records in response to a grand jury or law enforcement subpoena or to any judicial order or other lawfully issued subpoena, unless the issuer orders that notice not be given.[285]

Consequently, although the issue has not been decided by a court or in any formal manner by the U.S. Department of Education, a college or university is probably required under FERPA to use reasonable efforts to attempt to notify the student prior to disclosing education records in response to a new subsection (j) court order, unless the court's order commands that such notice not be given. Having reached this conclusion, it is important to note that the U.S. Department of Education in its April 12, 2002, "Dear Colleague" letter states that Section 507 of the USA PATRIOT Act permits a school to respond to a new subsection (j) court

282. USA PATRIOT Act § 507, 115 Stat. at 367–68 (codified at 20 U.S.C.A. § 1232g(j) (2000 & West Supp. 2003)).

283. "Notwithstanding" clauses in statutes do not "restrict the scope" of a provision but "designate[] the conditions in spite of which [they] apply." 1A NORMAN J. SINGER, STATUTES AND STATUTORY CONSTRUCTION § 21.12 (6th ed. 2002) (citing Beck v. Buena Park Hotel Corp., 196 N.E.2d 686 (Ill. 1964)).

284. USA PATRIOT Act § 507, 115 Stat. at 367–68 (codified at 20 U.S.C.A. § 1232g(j)) (adding subsection (j)(4) to 20 U.S.C. § 1232g). *See* 20 U.S.C.A. § 1232g(b)(4)(A) (2000).

285. USA PATRIOT Act § 507, 115 Stat. at 367–68 (codified at 20 U.S.C.A. § 1232g(j)) (adding subsection (j)(4) to 20 U.S.C. § 1232g).

order without first notifying the student.[286] The Department offers this advice without any analysis or justification, and for the reasons explained above, its conclusion does not appear to be a well founded construction of FERPA. It is possible, although not likely, that the Department means that Section 507 permits a court issuing a subsection (j) order to prohibit notice and, in such event, that FERPA would permit the school to comply and not give notice. In any event, all that the Department's Dear Colleague letter states is that a notice is not required.[287] So even under that guidance, it appears that a college or university may voluntarily give notice to a student prior to responding to a subsection (j) court order, unless the court has ordered that notice not be given. This ability to give notice is important for those schools whose internal policies and procedures would require notice to be given in the absence of a court or other lawful order or subpoena prohibiting notice. A school probably is prohibited from giving notice if a court issuing a subsection (j) court order orders that no notice be given.[288]

Although not addressed in the USA PATRIOT Act or in any other post-September 11 federal law, the Department of Education's April 12, 2002, "Dear Colleague" letter also provides guidance on the post-September 11 application of an existing exception to FERPA's prohibition against disclosure of education records without the student's prior written consent.[289] The "health or safety emergency" exception[290] allows a college or university to disclose education

286. Dear Colleague Letter, *supra* note 272, at 2.

287. *Id.*

288. Interestingly, subsection (b)(2)(B) of FERPA does not expressly provide that the lawful issuer of a court order may order a college or university not to give notice to a student before the college or university discloses education records. That authority is given by subsection (b)(1)(J), which applies only to the issuer of a grand jury or law enforcement subpoena. This subsection relating to other lawfully issued subpoenas and judicial orders, however, is administered in the same manner as subsection (b)(1)(J) relating to grand jury and law enforcement subpoenas (34 C.F.R. § 99.31(a)(9)(ii)), and it is likely that colleges or universities must comply with a subsection (b)(2)(B) judicial order that expressly prohibits the college or university from giving notice. This makes sense because it is not reasonable to conclude that the issuer of a subpoena for *any* law enforcement purpose, which may not even be a court, could prohibit a college or university from giving notice to the student, while a court that issues an order could not also prohibit notice. The case is made even more compelling when a court issues an order under subsection (j) in connection with the investigation of serious crimes of terrorism.

Federal law enforcement and Justice Department officials often "request" that notice not be given when a court order or subpoena they are executing does not expressly prohibit notice. Except to the extent that the Department of Education's Dear Colleague letter is correct with regard to subsection (j) orders, colleges or universities are prohibited by FERPA subsection (b) from acquiescing to such a request. A college or university, however, may explain the FERPA requirements, warn the government agent that the college and university will have to notify the student under the order or subpoena as initially issued, and give the government an opportunity to retract execution of the order or subpoena so that it may be reissued with an express prohibition against giving notice. *See* USA PATRIOT Act § 507, 115 Stat. at 367–68 (codified at 20 U.S.C.A. § 1232g(j) (2000 & West Supp. 2003)) (adding subsection (j)(4) to 20 U.S.C. § 1232g (2000) (no record keeping of educational records subject to court order required, notwithstanding subsection (b)(4)); 20 U.S.C.A. § 1232g(b)(2)(B) (2000); 34 C.F.R. § 99.31(a)(9)(ii) (2003).

289. Dear Colleague Letter, *supra* note 272, at 3–4.

290. 20 U.S.C.A. § 1232g(b)(1)(I) (2000); 34 C.F.R. § 99.31(a)(10).

records "to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals."[291] The Department's regulations, in a provision long predating the USA PATRIOT Act, points out that this exception is to be "strictly construed" and that the college or university must keep records of the disclosure.[292] There must be imminent danger to a student or others, only those with a need to know the information in the record to avert the emergency may be apprised of it, and the disclosure without consent is permitted only during the period when there is an immediate need to avert the health or safety emergency.[293] Consequently, the U.S. Department of Education points out that a college or university "has the responsibility to make the initial determination of whether a disclosure is necessary to protect the health or safety of the student or other individuals."[294] It should not be assumed that disclosure is necessary in every case involving a post-September 11 investigation. The college or university must undertake a thoughtful evaluation under the FERPA standard before determining whether to invoke this exception, even if federal law enforcement assumes the exception applies.[295] Of course, if federal law enforcement assert an emergency, it is prudent for the college or university to make its determination promptly under the circumstances.

V. USA PATRIOT ACT AMENDMENTS TO FEDERAL CRIMINAL INVESTIGATORY LAWS, EXPANDING FEDERAL LAW ENFORCEMENT'S POWERS

Title II of the USA PATRIOT Act[296] amends the U.S. Criminal Code,[297] the Foreign Intelligence Surveillance Act of 1978 ("FISA"),[298] and the National Security Act of 1947.[299] Title III of the USA PATRIOT Act[300] amends federal laws that govern banks and certain other financial institutions and are aimed at preventing them from facilitating money laundering for those who violate federal or international law.[301] Generally, these amendments expand law enforcement's

291. 34 C.F.R. § 99.36(a).

292. 34 C.F.R. §§ 99.32, 99.36(c).

293. *Id.*

294. Dear Colleague Letter, *supra* note 272.

295. *Id.* at 3 (examples of imminent threats justifying disclosure are disclosure of records to avert an anthrax, smallpox or other bioterror attack or to prevent another September 11 type of attack); 34 C.F.R. § 99.36(a), (c).

296. USA PATRIOT Act §§ 201–225, 115 Stat. 272, 278–96.

297. 18 U.S.C.A. §§ 2510–2522 (2000 & West Supp. 2003) (governing surveillance, search and seizure of wire (telephone) and electronic (e-mail) communications and oral communications); §§ 2701–2709 (2000 & West Supp. 2003) (the "Electronic Communications Privacy Act" governing surveillance, search and seizure of third-party stored wire and electronic communications and subscriber and customer records), §§ 3121–3127 (2000 & West Supp. 2003) (governing the use of pen registers and trap and trace devices to capture wire and electronic transmission and processing information).

298. 50 U.S.C.A. §§ 1801–1863 (2003 & West Supp. 2003).

299. 50 U.S.C.A. §§ 401–442 (2003 & West Supp. 2003).

300. USA PATRIOT Act §§ 301–377, 115 Stat. at 296–342.

301. 12 U.S.C.A. § 1829(b) (2001 & West Supp. 2003); 31 U.S.C.A. §§ 5311–5312, 5317–5319, 5321–5322, 5324, 5326, 5328, 5330–5332, 5341 (2003 & West Supp. 2003)).

authority to investigate federal crimes and to obtain information relevant to foreign intelligence, and enhance federal law enforcement's and intelligence agencies' ability to share information obtained in federal law enforcement and intelligence investigations. In certain circumstances, these amendments make electronic and other surveillance in connection with criminal and terrorism investigations easier for law enforcement by expanding the geographic jurisdiction of federal courts to issue search warrants, orders, and subpoenas for surveillance, searches, and seizures, and by providing avenues for using FISA instead of the U.S. Criminal Code, or for using less burdensome sections of the US Criminal Code than would otherwise apply to some investigations. Whether or not FERPA applies, colleges and universities should be prepared to review subpoenas, court orders, and search warrants for their sufficiency and to make appropriate inquiries of law enforcement officials about the underlying basis for their issuance before responding.[302] The present article will address the highlights of the changes that expand federal law enforcement's investigatory and information sharing powers, and will put these changes into the context of the laws they amend. For a detailed review of the USA PATRIOT Act amendments to these federal criminal laws and to the federal laws that protect against money laundering, refer to *The USA PATRIOT Act: A Legal Analysis*[303] and to the separate article[304] in this Symposium on amendments to money laundering and other laws governing a wide range of financial and related activities.

The U.S. Criminal Code establishes conditions to federal law enforcement's surveillance, search, and seizure of telephone or wire, in person, and electronic (e-mail) communications and records, with the degree of burden imposed on law enforcement varying in accordance with the type of information sought and whether there is a reasonable expectation of privacy in the information. The conditions imposed by the U.S. Criminal Code are intended to satisfy the requirements of the Fourth Amendment to the Constitution, protecting against unreasonable searches and seizures, and, even where no Fourth Amendment interest exists, to provide for the important interest of free expression of information among private parties.[305]

302. Court orders under these provisions of the U.S. Criminal Code are issued *ex parte*, without the target being represented at a hearing prior to issuance, and federal law enforcement usually will not be able or willing to divulge the factual basis. Institutions should still review the statutory requirements with the executing federal law enforcement official and seek assurance from the official that the requirements were met. The college and university should document this process and the assurances received in a memorandum to the file. Such review may divulge the need for law enforcement to take further steps before executing an order or subpoena and will provide the college and university with some evidence of having been reasonable to ensure that it is responding appropriately to a lawfully issued order or subpoena and that the order or subpoena is in fact lawfully issued.

303. Doyle, *supra* note 10.

304. Larose, *supra* note 12.

305. Doyle, *supra* note 10, at 2–4, notes 6–8 (describing these conditions as they relate to "three tiers" of the U.S. Criminal Code, each relating to a different category of intrusion and each imposing a different level of protection, and noting that some communications such as telephone records and e-mail held by third parties are not protected by the Fourth Amendment); Bartnicki v.

As is discussed in greater detail in the following Parts of this article, the greatest protection is accorded under the Fourth Amendment and the U.S. Criminal Code to oral (in-person), wire (telephone), and, to a slightly lesser extent, electronic (e-mail) communications, including content, as they occur. Interception of oral and wire communications requires a court order with probable cause to believe that the information sought is evidence concerning any of a specified list of federal crimes and that there is no feasible alternative to the proposed interception (among other findings), upon an application filed with approval by a senior Justice Department attorney. In the case of interceptions of e-mail, a court order with probable cause to believe that the information sought is relevant to any federal felony is required upon an application, but one that does not by statute require Justice Department approval.[306] Unopened electronic and wire (voicemail) communications (including content) stored by third-party service or storage providers for 180 days or less are provided a significant, albeit a somewhat lesser, level of protection. Unless the subscriber to the service or the sender or intended recipient of such communication consents to the disclosure, a search warrant is still required, but the court need only find that there is probable cause to believe that the information sought will provide evidence of any crime being investigated, and there is no need for a senior Justice Department attorney's approval of the application.[307] Electronic and wire transmission and processing information (such as telephone numbers, e-mail addresses, and routing, signaling, and processing information, but not content) are also accorded a significant, but lesser, amount of protection under the U.S. Criminal Code. Interceptions of this information require an authorizing court order on a finding of relevance to an ongoing criminal investigation.[308] Unopened wire (voicemail) and electronic (e-mail) communications stored by third-party service providers for more than 180 days, all opened communications, and service records (such as certain subscriber and customer identification, service, and billing information, but not content) are accorded a lower level of protection. Search and seizure of these communications and records may be authorized through a variety of means. An administrative agency subpoena authorized by any federal or state law, a trial court or grand jury subpoena routinely issued upon request by an assistant U.S. attorney or district attorney, or consent of the subscriber, sender or intended recipient, none of which require court approval, will suffice. A court order on reasonable grounds to believe that the information is relevant to an ongoing criminal investigation also may authorize such activities.[309] FISA provides for the most secret U.S. court-authorized electronic, wire, and physical searches and seizures, and provides for "dual purpose" investigations

Vopper, 532 U.S. 514 (2001) (concerning Title III); James A. Adams, Commentary, *Pen Registers and Trap and Trace Devices,* 18 U.S.C.S. ch. 206, at 121–23 (LEXIS Supp. 2003) (Lawyer's Edition) (when the Supreme Court held that there is no reasonable expectation of privacy and thus no Fourth Amendment interest in telephone numbers, Congress determined to regulate the use of pen registers and trap and trace devices).

306. *See infra* Part V.1.

307. *See infra* Part V.2.

308. *See infra* Part V.3; Adams, *supra* note 305, at 121–23.

309. *See infra* Part V.2.

where a significant purpose is intelligence gathering.[310]

1. Contents of Telephone, Oral, and E-mail Communications as They Occur

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III")[311] imposes the greatest protections of individual privacy on federal law enforcement's criminal investigations. This portion of the U.S. Criminal Code relates to what are commonly known as "wiretaps" and federal law enforcement's ability to seize the content of oral, wire, and electronic communications in which there is an expectation of privacy, including the content of private conversations over the telephone, in person, and in e-mail, as they occur.[312]

Under Title III, federal law enforcement is prohibited from intercepting telephone (wire), in person, or other oral communications as they occur unless a court issues an *ex parte* order authorizing such surveillance.[313] The order is issued only in response to federal law enforcement's application, after a Deputy Assistant Attorney General or higher Justice Department official designated by the Attorney General first approves the application.[314] To justify the Attorney General's approval of the application and the court's issuance of the order, each must find that there is probable cause to believe the surveillance "may provide or has provided" evidence of a list of federal crimes specified in the statute.[315] Provisions of the USA PATRIOT Act that sunset on December 31, 2005, expand this list of crimes to include crimes of domestic and international terrorism and certain cyber crimes.[316]

To obtain an authorizing order, federal law enforcement must submit an application to the court that includes "a full and complete statement of facts and

310. *See infra* Part V.6. For a quick reference table summarizing generally the requirements for obtaining each type of information or property under the U.S. Criminal Code, as well as under FISA, see The Search & Seizure of Electronic Information: The Law Before and After the USA PATRIOT Act, available at http://www.ll.georgetown.edu/aallwash/uspatriotbefaft.pdf.

311. Pub. L. No. 90-351, 82 Stat. 237 (1968) (codified as amended at 18 U.S.C.A. §§ 2510–2522 (2000 & West Supp. 2003)).

312. *Id.* Wiretap is too narrow a term to accurately describe the reach of Title III, as it applies to the government's ability to seize, listen to and access the content of electronic (e-mail) communications as well as oral and telephone or other wire communications. It is beyond the scope of this article to address the different analysis that applies to wireless telephones such as cell phones.

313. 18 U.S.C.A. § 2511 (2000 & West Supp. 2003) (prohibiting interception of wire and oral communications); § 2516 (2000 & West Supp. 2003) (providing for an *ex parte* court order to authorize interception of wire and oral communications that "may provide or [have] provided evidence" of any of the federal crimes listed in this section), § 2518 (2000) (specifying the procedure for securing such court order, including the required content of the application and the required probable cause findings by the court).

314. *Id.* § 2516 (2000 & West Supp. 2003).

315. *Id.* (requiring the finding regarding evidence of federal crimes and listing the federal crimes covered).

316. USA PATRIOT Act § 201, 115 Stat. 272, 278 (codified at 18 U.S.C.A. § 2516); § 202, 115 Stat. at 278 (codified at 18 U.S.C.A. § 2516); § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note (2000 & West Supp. 2003). *See* Doyle, *supra* note 10, at 8.

circumstances" justifying the issuance of the order and supporting a finding "as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed . . . or [are] too dangerous."[317] To issue the order authorizing the surveillance, the court must find that there is probable cause to conclude that one of the specified crimes is being or has been committed,[318] that evidence of the crime "will be obtained" through the surveillance,[319] that "normal investigative procedures have been tried and failed or reasonably appear unlikely to succeed or [are] too dangerous,"[320] and, with certain exceptions, that the facilities where the interception will occur or from which the communications to be intercepted will be transmitted are involved in the crime or are used, owned, or controlled by the person committing the crime.[321] The findings concerning facilities are not required (and a so-called "roving" order may issue allowing the interception to follow the target) in the case of an application to intercept oral communications, if the U.S. Attorney General, Deputy Attorney General, Associate or Assistant Attorney General approves the application[322] and the application provides adequate support for the conclusion that specifying the facilities is not practical (among other findings)[323] and the court so finds.[324] The facilities findings also are not required, and a roving order may issue, in response to an application relating to wire (telephone) communications, if the application provides adequate support for the finding that the target's "actions could have the effect of thwarting interception from a specified facility"[325] and that the time for interception is limited to the time when the target "is or was reasonably proximate to the [transmitting] instrument" (among other findings) and the court so finds.[326]

A court may issue such an *ex parte* order to authorize interception of electronic (e-mail) communications as they occur, on the same findings and subject to the same procedures as apply to oral and wire communications, with two exceptions. An order authorizing the interception of e-mail may, by statute, be based on an application submitted by federal law enforcement without approval of the application by the designated high level senior Justice Department attorneys, and such order may be issued in connection with any federal felony investigation (not only the listed federal crimes that apply to oral and wire communications).[327] The findings concerning facilities are not required for electronic communications (and a roving order may issue) in the same circumstances and under the same conditions as such findings are not required (and a roving order may issue) for wire

317. 18 U.S.C.A. § 2518(1)(c) (2000).
318. *Id.* § 2518(3)(a) (2000).
319. *Id.* § 2518(3)(b) (2000).
320. *Id.* § 2518(3)(c) (2000).
321. *Id.* § 2518(3)(d) (2000).
322. *Id.* § 2518(11)(a)(i) (2000).
323. *Id.* § 2518(11)(a)(ii) (2000).
324. *Id.* § 2815(11)(a)(iii) (2000).
325. *Id.* § 2518(11)(b)(ii) (2000).
326. *Id* § 2518(11)(b)(iii) (2000).
327. *Id.* §§ 2516(3), 2518(7) (2000).

communications.[328] In addition, a provision of the USA PATRIOT Act that sunsets on December 31, 2005, authorizes federal law enforcement, without any court authorization, to seize the communications to and from a person who breaches another person's computer system, provided that the owner of the compromised computer system authorizes the interception and only the trespassing person's communications are seized.[329]

All such court orders, whether for interception of wire, oral, or electronic communications, limit the scope and duration of the surveillance and may include close supervision by the court through required periodic reports.[330] Title III orders are the most burdensome on law enforcement, particularly in light of the degree of court supervision that may apply and because such orders for oral and wire (telephone) communications may be sought only in connection with specified federal crimes. The USA PATRIOT Act's provision of opportunities to seek FISA orders or other U.S. Criminal Code orders in certain circumstances in lieu of Title III orders facilitates law enforcement's investigations and shifts the balance of individual rights and law enforcement's powers.[331]

2. Telephone and E-mail Subscriber Records and Stored Records of E-mail and Telephone Content

Supplementing Title III of the U.S. Criminal Code is the Electronic Communications Privacy Act ("ECPA"),[332] which generally prohibits unauthorized access to, or disclosure by e-mail and voicemail service providers "to the public"[333] of any e-mail or voicemail stored by such service providers. The ECPA has always covered e-mail, and a provision of the USA PATRIOT Act that sunsets on December 31, 2005, expands the ECPA's coverage to stored wire communications, such as voicemail.[334] The ECPA provides for federal and state

328. *Id.* § 2518(3), (11) (2000).

329. USA PATRIOT Act § 217, 115 Stat. 272, 290–91, 295 (codified at 18 U.S.C.A. §§ 2510–2511 (2000 & West Supp. 2003); § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note (2000 & West Supp. 2003)). *See* Doyle, *supra* note 10, at 8.

330. 18 U.S.C.A. § 2518(5)–(11) (2000 & West Supp. 2003). *See* Doyle, *supra* note 10, at 2–4 & n. 8, 8 & nn. 16–17 (standard for finding by the court).

331. *See* USA PATRIOT Act § 214, 115 Stat. at 286–87 (amending 50 U.S.C. §§ 1842–1843).

332. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C.A. §§ 2510–2520 (2000 & West Supp. 2003)) [hereinafter ECPA].

333. *Id.* § 102, 100 Stat. at 1853 (codified at 18 U.S.C.A. § 2511(3) (2000 & West Supp. 2003)).

334. USA PATRIOT Act § 209, 115 Stat. at 283 (amending 18 U.S.C. §§ 2510, 2703). The ECPA applies to "provider[s] of electronic communication services" and "provider[s] of remote computing services," but only if the services are offered "to the public." ECPA § 201, 100 Stat, at 1860–61 (codified at 18 U.S.C.A. § 2702 (2000 & West Supp. 2003)). These statutory provisions raise several different issues: What is the difference between an electronic communication service and a remote computing service? Do colleges and universities that make such services available incident to their core educational purposes qualify as "providers" for the purpose of the ECPA? If they do, are their services made available "to the public"?

The terms "electronic communication service" and "remote computing service" date

law enforcement and other government officials to search and seize wire

back to the passage of the ECPA in 1986, and reflect a now somewhat archaic distinction between two functions that are typically carried out by entities operating e-mail and voicemail services: an e-mail or voicemail message, until it is opened, is part of an electronic communication service; once opened, and if left on the system, it becomes part of a remote computing service. H.R. REP. NO. 99-647, at 64–65 (1986). *See also* In re Doubleclick, Inc. Privacy Litigation, 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (a message is in an electronic communication service for the purposes of the ECPA only until it is read). Entities that operate such services only incidental to the entities' other activities are nonetheless providers covered by the ECPA. *See, e.g.,* Bohack v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (city is provider of electronic communication services in operating paging service for its police department).

Whether such services are offered "to the public," simply because members of the college's or university's community can receive or send messages to the public, is unclear. The only court decision that has expressly addressed the issue is *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998), which held that a private entity's internal e-mail system was not an electronic communication service provided "to the public" simply because outsiders could send e-mails to or receive e-mails from employees using the employer's internal e-mail system. But the Computer Crime and Intellectual Property Section of the Criminal Division of the United States Department of Justice has issued a guideline, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Sec. III.B* (July 2002), *available at* http://www.cybercrime.gov/s&smanual2002.htm (last visited Apr. 4, 2004), that takes the position that private employers' e-mail systems are electronic communication services "to the public" for messages received by employees from outsiders, until they are read. That guideline concludes, however, that, once read, the message on the system is treated as in a remote computing service, and in the case of a private employer, that such a remote computing service is not available "to the public," and therefore not subject to the ECPA.

The complexity of the ECPA and the lack of clear authority for interpreting the terms it uses, coupled with the fact that college and university e-mail and voicemail systems are used so broadly by others than faculty, staff and enrolled students (e.g., visiting scholars, alumni/ae, enrichment and continuing education program participants, research subjects, etc.), support the conclusion that it is prudent for a college or university to interpret the ECPA as applying to all communications on its e-mail and voicemail systems, whether opened or unopened, until otherwise advised by a court that has considered the institution's particular situation.

The USA PATRIOT Act amends the ECPA. USA PATRIOT Act § 209, 115 Stat. at 283 (amending 18 U.S.C. 2703 to cover both stored wire (voicemail) as well as stored electronic (e-mail) communications and treating voicemail as e-mail, rather than as a telephone communication, for search and seizure purposes); § 210, 115 Stat. at 283 (amending 18 U.S.C. § 2703(c)(2) to expand the information that may be seized, including credit card and bank account numbers); § 211, 115 Stat. at 283-84 (amending § 631 of the Communications Act of 1934, 47 U.S.C. § 551, to provide for the easier-to-satisfy ECPA requirements to apply to search and seizure of telephone and e-mail service-related information when cable companies are telephone and/or e-mail service providers, while confirming that the harder-to-satisfy Communications Act of 1934 requirements continue to govern cable television programming-related records); § 220, 115 Stat. at 291-92 (amending 18 U.S.C. § 2711 to define "court of competent jurisdiction" as any federal court with jurisdiction over the crime being investigated without regard to such court's otherwise applicable geographic limitations, for authorizing search and seizure of records under 18 U.S.C. § 2703(c) and e-mail and voicemail stored by third parties for more than 180 days under 18 U.S.C. § 2703(b)); Doyle, *supra* note 10, at 4, 6–8; Adams, *supra* note 305, at 121–23; Sections 209 and 220 sunset on December 31, 2005, but Sections 210 and 211 do not. USA PATRIOT Act § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note). *See* 18 U.S.C.A. §§ 2701-2702 (2000 & West Supp. 2003) (prohibiting interception and disclosure except as otherwise provided); § 2711 (incorporating the definitions in 18 U.S.C.A. § 2510 (2000 & West Supp. 2003)).

(telephone) and electronic (e-mail) service records and/or stored communications in connection with the investigation or prosecution of any crime, subject to a range of protective conditions depending on the level of information sought.[335] In particular, ECPA concerns the government's ability to search and seize telephone and e-mail records ranging from subscriber information (meaning the name, address, account identifiers, and other specified information about the subscriber or customer of telephone or e-mail service), to the contents of telephone voicemail and e-mail communications stored electronically by third-party service providers. A provision of the USA PATRIOT Act that sunsets on December 31, 2005, also expands the geographic reach of the federal courts' jurisdiction to issue certain of these authorizing orders to nationwide jurisdiction.[336]

If the government seeks to search and seize unopened e-mail or wire (voicemail) communications (including content) stored electronically by providers of electronic communications or storage services, different rules generally apply to content stored for 180 days or less from those that apply to content stored for more than 180 days.[337] If the sender or intended recipient of the communication or the subscriber of storage services lawfully consents to the disclosure, however, e-mail and voicemail content stored for any period may be disclosed without any court authorization.[338]

To access unopened e-mail and voicemail that have been stored for 180 days or less by a third party, including a college or university, that provides e-mail and voicemail communications and/or storage service, the government must obtain a search warrant issued under procedures established in the Federal Rules of Criminal Procedure, or an equivalent state law warrant, by a court with jurisdiction

335. ECPA § 201, 100 Stat. at 1861–63 (codified at 18 U.S.C.A. § 2703 (2000 & West Supp. 2003)).

336. USA PATRIOT Act § 220, 115 Stat. at 291–92 (amending 18 U.S.C. § 2711 to define "court of competent jurisdiction" for purposes of authorizing seizure of unopened e-mail and voicemail stored for more than 180 days by a third-party service provider under 18 U.S.C. § 2703(b) and seizure of service records under 18 U.S.C. § 2703(c) to include federal courts with jurisdiction over the crime being investigated without regard to such courts' otherwise applicable geographic limitations); 18 U.S.C.A. § 2703(a) (2000 & West Supp. 2003) (government access to e-mail and voicemail electronically stored for 180 days or less), (b) (government access to unopened e-mail and voicemail electronically stored for over 180 days and all opened e-mails and accessed voicemails), (c) (government access to subscriber telephone and electronic communications service records). Interception of telephone and e-mail communications, as they are occurring, is subject to 18 U.S.C.A. § 2703. *See supra* Part V.1 and notes 312–16.

337. 18 U.S.C.A. § 2703(a) (unopened e-mail and voicemail stored 180 or fewer days), (b) (unopened e-mail and voicemail stored over 180 days and all opened e-mails and accessed voicemails) (2003); Doyle, *supra* note 10, at 4, 6 (citing 18 U.S.C. § 2703(a)–(b) (2000)). With the USA PATRIOT Act amendments (Sections 209 and 220) to 18 U.S.C. §§ 2703 and 2711, law enforcement has access through 18 U.S.C.A. §§ 2701–2711 (2000 & West Supp. 2003) to the content of third-party stored telephone voicemail in connection with any crime, not only in connection with the Title III crimes listed in 18 U.S.C.A. § 2516 (2000 & West Supp. 2003), and federal courts' geographic jurisdiction to issue authorizing orders is nationwide. *See supra* notes 334–36; Doyle, *supra* note 10, at 7.

338. 18 U.S.C.A. § 2702(b)(3) (2000). Subsection 2702(b) provides other exceptions to the nondisclosure rule as well.

over the crime being investigated.[339] Thus the court must find probable cause that the content being sought will provide evidence of the crime being investigated and over which the court has jurisdiction.[340]

To access e-mails that have been opened or voicemails that have been accessed, as well as unopened e-mail and voicemail that have been stored for over 180 days by a third-party service provider, the government must obtain either (a) a search warrant issued using the procedures described in the Federal Rules of Criminal Procedure or an equivalent state warrant, with probable cause by "any court of competent jurisdiction," which will not require notice to the subscriber or customer, or (b) a court order issued by "any court of competent jurisdiction," an administrative agency subpoena authorized by a federal or state statute, or a grand jury or trial court subpoena (routinely issued upon request by a government attorney), all of which will require notice to the subscriber or customer.[341] A court may authorize delaying notice for up to ninety days if it finds that the government provided adequate evidence that there would be an adverse result (e.g., a person would be physically endangered, a target might flee, or evidence might be destroyed) if notice were given.[342] A court order for contents of opened e-mail or accessed voicemail, or for unopened e-mail or voicemail held for more than 180 days, must be based on "articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation."[343] A search warrant must be based on probable cause to believe that the information sought will provide evidence of a crime.[344]

339. *Id.* § 2703(a) (2000 & West Supp. 2003).

340. *Id.*; USA PATRIOT Act §§ 209, 220(a)(1), 115 Stat. at 283, 291–92 (amending 18 U.S.C. § 2703(a)). *Cf.* FED. R. CRIM. P. 41(f) (requiring copy of a warrant to be provided to the party from whom or whose property is being seized). Sections 209 and 220 sunset on December 31, 2005. *See* USA PATRIOT Act § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

341. USA PATRIOT Act § 209, 115 Stat. at 283 (amending 18 U.S.C. § 2703(b)); § 212, 115 Stat. at 284-85 (amending 18 U.S.C.A. § 2703); § 220(a)(1), 115 Stat. at 291-92 (amending 18 U.S.C. § 2703(b)); § 213, 115 Stat. at 285–86 (amending 18 U.S.C. § 3103a) (generally authorizing delaying notice of any orders on a showing of adverse results); 18 U.S.C.A. §§ 2703(a)–(b), (d), 2705 (2000 & West Supp. 2003). *See infra* Part V.4. Sections 209, 212, and 220 of the USA PATRIOT Act sunset on December 31, 2005, but Section 213 does not. *See* USA PATRIOT Act § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

Note that another provision of the USA PATRIOT Act that does not sunset, § 213, 115 Stat. at 285-86, amends 18 U.S.C. § 3103a to permit a delay in the case of a search warrant or related court order (issued under FED. R. CRIM. P. 41(b) or "any other rule of law") of unspecified duration "of any notice required, or that may be required to be given," on a finding that an "adverse result" would arise from earlier notice. *See infra* Part V.4 and note 372. This more open-ended authority to delay notice requirements imposed by other laws or rules if a search warrant is used contrasts with the more restricted authority to delay notice when a court order under 18 U.S.C. § 2703(b) is used.

342. USA PATRIOT Act § 213, 115 Stat. at 285–86 (codified at 18 U.S.C.A. § 3103a(b) (2000 & West Supp. 2003)).

343. 18 U.S.C.A. § 2703(d) (2000 & West Supp. 2003).

344. FED. R. CRIM. P. 41(d)(1).

With the USA PATRIOT Act amendments, a "court of competent jurisdiction" includes a state court with general criminal jurisdiction under state law or any federal district court, magistrate, or appeals court with jurisdiction over the crime, without regard to such federal court's otherwise applicable geographic limitations.[345] Consequently, until December 31, 2005, when the relevant section sunsets, the USA PATRIOT Act expands the geographic jurisdiction of federal courts to issue court orders for e-mail and voicemail content.[346]

A provision of the USA PATRIOT Act that sunsets on December 31, 2005, also authorizes electronic communications service and storage service providers to voluntarily disclose the contents of stored e-mail and voicemail, whether opened or unopened, "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay."[347] In addition, this provision of the USA PATRIOT Act authorizes such service providers to voluntarily disclose to any government entity, service records of or other information pertaining to a subscriber or customer, but not content, if the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information."[348] These are voluntary disclosures, not required disclosures, and providers must make their own determinations of whether it is appropriate or advisable to make any such disclosures taking into account the particular circumstances as they arise.

If the government seeks merely subscriber or customer service records, but not the stored content of e-mail and telephone communications, the government must obtain authorization (a) by lawful consent of the subscriber or customer,[349] (b) by a warrant issued using the procedures established under the Federal Rules of Criminal Procedure by a court having jurisdiction over the crime being investigated or an equivalent state warrant[350] (including, under a provision of the USA PATRIOT Act that sunsets on December 31, 2005, any federal court with jurisdiction over the crime being investigated without regard to its otherwise applicable geographic limitations),[351] (c) by a court order issued by any "court of competent jurisdiction"[352] (including, under a provision of the USA PATRIOT Act

345. USA PATRIOT Act § 220(a)(2)(C), 115 Stat. at 292 (amending 18 U.S.C. § 2711).

346. *See id.* § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

347. *Id.* § 212(a)(1)(D), 115 Stat. at 284 (amending 18 U.S.C. § 2702(b)(6) by adding a new subsection (C)); § 212(a)(1)(E), 115 Stat. at 284-85 (amending 18 U.S.C. § 2702 by adding new subsection (c)(4)). This section of the USA PATRIOT Act sunsets on December 31, 2005. *See id.* § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

348. *Id.* § 212(a)(1)(D), 115 Stat. at 284 (amending 18 U.S.C. § 2702(b)(6) by adding a new subsection (C)). Content may be obtained under 18 U.S.C.A. § 2702(b)(6) (2000 & West Supp. 2003). *See supra* note 347. These sections of the USA PATRIOT Act sunset on December 31, 2005. *See* USA PATRIOT Act § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

349. 18 U.S.C.A. § 2703(c)(1)(C) (2000 & West Supp. 2003).

350. *Id.* § 2703(c)(1)(A) (2000 & West Supp. 2003).

351. USA PATRIOT Act § 220(a)(3), 115 Stat. at 292 (amending 18 U.S.C. § 3127).

352. 18 U.S.C.A. § 2703(c)(1)(B) (2000 & West Supp. 2003). For the definition of "court of competent jurisdiction," see *supra* note 343, and USA PATRIOT Act § 220(a)(1), (3), 115 Stat. at

that sunsets on December 31, 2005,[353] any federal court with jurisdiction over the crime being investigated without regard to its otherwise applicable geographic limitations),[354] or (d) by an administrative agency subpoena authorized by a federal or state law or by a federal or state grand jury or trial subpoena.[355] Any such warrant, order, or subpoena will issue without any requirement for notice to the subscriber or customer,[356] and may authorize the search and seizure of certain subscriber or customer information. Previously such information included the subscriber or customer name, address, local and long distance telephone billing records, telephone number or other subscriber or customer name or number, and length and type of service.[357] With USA PATRIOT Act amendments that do not sunset, the previously accessible information continues to be accessible, and telephone connection records, records of service use, times and durations, date when telephone or e-mail service was initiated, temporary network addresses, and means and source of payment for telephone or e-mail service, including credit card or bank account number, are accessible as well.[358] Any such subpoena may not authorize access to content and will be issued on an offer of "specific and articulable facts showing . . . reasonable grounds to believe that the . . . records . . . sought, are relevant and material to an ongoing criminal investigation."[359]

3. Pen Registers and Trap and Trace Devices in Criminal Investigations

Under another portion of the U.S. Criminal Code, the use of pen registers and trap and trace devices in connection with wire (telephone) and electronic (e-mail) communications is prohibited unless an authorizing court order is first obtained.[360] When authorized to use these registers and devices, they must be used to obtain the limited transmission information authorized about wire and electronic communications, and such information may not include content or billing information. The information that may be authorized by such an order is the identifying name or number and electronic and other impulses of the source of a transmission and the dialing, routing, addressing, and signaling information transmitted.[361] A provision of the USA PATRIOT Act that does not sunset

291–92 (amending 18 U.S.C. §§ 2703, 2711).

353. *See* USA PATRIOT Act § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note (2000 & West Supp. 2003)).

354. *Id.* § 220(a)(3), 115 Stat. at 292 (amending 18 U.S.C. § 3127).

355. 18 U.S.C.A. § 2703(c)(2) (2000 & West Supp. 2003).

356. 18 U.S.C.A. § 2703(c)(3) (2000 & West Supp. 2003).

357. *Id.* § 2703(c)(1)(C) (2000 & West Supp. 2003).

358. *Id.* § 2703(c)(1)–(2) (2000 & West Supp. 2003); USA PATRIOT Act § 210, 115 Stat. at 283 (amending 18 U.S.C. § 2703(c)(2)). Section 210 of the USA PATRIOT Act does not sunset on December 31, 2005. *See id.* § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note). *See also* Doyle, *supra* note 10, at 6.

359. 18 U.S.C.A. § 2703(d).

360. *Id.* §§ 3121–3127, 3121(a) (2000 & West Supp. 2003) (requiring an order under Section 3123 or FISA, 50 U.S.C.A. §§ 1801–1863 (2003 & West Supp. 2003)).

361. USA PATRIOT Act § 216(c)(2)–(3), 115 Stat. at 290 (2000 & West Supp. 2003) (amending 18 U.S.C. § 3127, which defines pen registers and trap and trace devices and what they may and may not capture). Section 216 of the USA PATRIOT Act does not sunset on

amends the statute to ensure that this limitation is met, while also expanding the information authorized by the statute to be captured and the object of the installation to include both transmission devices, as well as processes (e.g., software), and to include facilities as well as instruments. This provision of the statute, as amended by the USA PATRIOT Act, requires the use of technology that is "reasonably available . . . [and] restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing and signaling information utilized in the processing and transmitting of wire [telephone] or electronic communications so as not to include the contents . . . ."[362]

Under a provision of the USA PATRIOT Act that does not sunset, the geographic reach of the court order and of the issuing court's jurisdiction is greatly expanded from the usual geographic jurisdiction of the court to nationwide, when a government attorney (meaning the Attorney General, any U.S. Attorney, any authorized Assistant Attorney General or Assistant U.S. Attorney, and any other federal attorney authorized to act as prosecutor under the federal rules applies for the order).[363] When a government attorney applies for an order to any federal court of competent jurisdiction, the court will issue an *ex parte* order authorizing law enforcement officials to use pen registers and trap and trace devices "anywhere within the United States," and the order may be served upon and apply to any individual or entity who provides wire or electronic communication service in the United States and who can assist in the execution of the order.[364] When state investigative or law enforcement officers apply for the order, the court will issue an *ex parte* order authorizing law enforcement officials to use pen registers and trap and trace devices "within the jurisdiction of the court."[365]

The USA PATRIOT Act amends the definition of "court of competent jurisdiction" that can issue these orders in the case of federal courts, to any court with jurisdiction over the crime, without regard to otherwise applicable geographic limitations, expanding such courts' geographic reach to nationwide. The definition

December 31, 2005. *See id.* § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

362. *Id.* § 216(a)(3), 115 Stat. at 288 (2000 & West Supp. 2003) (amending 18 U.S.C. § 3121(c)); § 216(c)(2)–(3), 115 Stat. at 290 (2000 & West Supp. 2003) (amending 18 U.S.C. § 3127 to add "process" and "facility" to device and instrument in the definition of pen registers and to add "process" to the definition of trap and trace devices); Adams, *supra* note 305, at 121–23.

363. USA PATRIOT Act § 216(b)(1), 115 Stat. 288–89 (federal government attorney applications for an *ex parte* order) (amending 18 U.S.C. § 3123(a)); 18 U.S.C.A. § 3122 (2000) (applications); 18 U.S.C.A. § 3127(5) (2000 & West Supp. 2003) (defining government attorneys as they are defined in the federal rules of criminal procedure); FED. R. CRIM. P. 1(b)(1). Section 216 of the PATRIOT Act does not sunset on December 31, 2005. *See* USA PATRIOT Act § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

364. USA PATRIOT Act § 216(b)(1), 115 Stat. at 288–89 (2000 & West Supp. 2003) (amending 18 U.S.C. § 3123(a)). Section 216 of the PATRIOT Act does not sunset on December 31, 2005. *See id*. § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

365. *Id.* § 216(b)(2), 115 Stat. at 288–89 (amending 18 U.S.C. § 3123(a)). Section 216 of the PATRIOT Act does not sunset on December 31, 2005. *See id*. § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

remains the same for state courts, i.e., any state court of "general criminal jurisdiction . . . authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device."[366] To issue the order, the court must find that it has received the required application, including a certification of a state or federal government attorney or a state law enforcement officer (unless barred by state law), that the information likely to be obtained "is relevant to an ongoing criminal investigation" being conducted by the agency identified in the application.[367]

The order authorizing a pen register or trap and trace device must be sealed by the court, and the owner of the line or other facility to which the register or device will be attached is prohibited from disclosing its existence to the subscriber or any other person, and must provide assistance to the executing officer as unobtrusively as possible and so as not to interfere with the service being provided if possible.[368] The person or entity on whom an order issued by a federal court will be served need not be specified in the order; however, the executing officer is required to give a "written or electronic certification that the order applies" to a person or entity when the person or entity who is not specifically named is served with the order, and requests such certification.[369] It is wise to request this certification to document that the court order to install, or assist in installing, the register or device applies to the institution.[370]

4. Expanding Federal Court Jurisdiction to Issue Search Warrants in Terrorism Investigations and Authority to Delay Notices of Searches and Seizures

The USA PATRIOT Act facilitates searches and seizures in terrorism investigations by amending the Federal Rules of Criminal Procedure to broaden the jurisdiction of federal magistrates to issue search warrants. A provision of the Act that does not sunset authorizes a federal magistrate judge in any judicial district to issue a search warrant on a finding of probable cause that evidence of a crime of domestic or international terrorism will be found, relating to any property or person wherever the target of the warrant is located, whether inside or outside of

366. *Id.* § 216(c)(1), 115 Stat. at 290 (amending 18 U.S.C. § 3127(2)(A) (federal district court, magistrate, or appeals court, or state court with general criminal jurisdiction and jurisdiction to authorize pen registers and trap and trace devices); 18 U.S.C.A. § 3127(2)(B) (2000 & West Supp. 2003).

367. USA PATRIOT Act § 216(b)(1), 115 Stat. at 289 (amending 18 U.S.C. 3123(a)).

368. 18 U.S.C.A. §§ 3123(d), 3124(a)–(b) (2000 & West Supp. 2003).

369. USA PATRIOT Act § 216(b), 115 Stat. at 288–89 (amending 18 U.S.C. § 3123(a)(1)). *See also* Doyle, *supra* note 10, at 4–5, note 10 (addressing 18 U.S.C.A. §§ 3123–3127 (2000 & West Supp. 2003)). USA PATRIOT Act § 216(c), 115 Stat. at 290, amends 18 U.S.C. § 3127(2) to define "court of competent jurisdiction" for purposes of 18 U.S.C. §§ 3123–3127 to mean "any district court of the United States . . . (including a magistrate judge . . .) or any United States court of appeals having jurisdiction over the offense being investigated."

370. *See supra* Part IV (concerning FERPA). Some of the types of information that may be intercepted through a pen register or trap and trace device may qualify as "education records" under FERPA. If the information may relate in part to any student, it is prudent, and may be necessary, to obtain a court order prohibiting notice that otherwise would be required by FERPA.

the magistrate's federal district.[371]

In addition, a provision of the USA PATRIOT Act that does not sunset supplements the Federal Rules of Criminal Procedure by allowing a delay in giving any notice required by law in connection with a search warrant or related court order issued under the Federal Rules of Criminal Procedure or "any other rule of law" for a search or seizure in connection with gathering evidence of violations of any federal law. To justify a delay, the court must find that there is reason to believe "that providing immediate notification of the execution of the warrant may have an adverse result," tangible property must not be seized unless the court finds a reasonable necessity of such seizure, and the court must provide for notice to be given within a reasonable, but extendable, time after the execution of the warrant or related court order.[372]

5. Sharing of Grand Jury, Criminal Investigatory, and Intelligence or Counterintelligence Information

The USA PATRIOT Act enhances the ability of federal law enforcement, immigration, and foreign intelligence agencies, among other federal agencies, to share criminal investigatory information that may be useful in matters involving foreign intelligence and counterintelligence, and in some cases, national defense or security.[373]

A provision of the USA PATRIOT Act that does not sunset on December 31,

371. USA PATRIOT Act § 219, 115 Stat. at 291 (amending FED. R. CRIM. P. 41(a)). Section 219 does not sunset. *See id.* § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

372. *Id.* § 213, 115 Stat. at 285–86 (amending 18 U.S.C. § 3103a, which supplements FED. R. CRIM. P. 41(b)). Section 213 does not sunset. *See id.* § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note). For the definition of "adverse result," see 18 U.S.C.A. § 2705(a)(2) (2000 & West Supp. 2003) and USA PATRIOT Act § 213(2), 115 Stat. at 286 (e.g., a person would be physically endangered, a target might flee, or evidence might be destroyed).

373. USA PATRIOT Act § 203, 115 Stat. at 278–81 (codified at scattered sections of 18 and 50 U.S.C.A., and 18 U.S.C.A. FED. R. CRIM. P. 6). USA PATRIOT Act § 203(a) (relating to sharing grand jury information) and (c) (requiring the Attorney General to develop rules to identify United States persons under FISA, 50 U.S.C. § 1801) do not sunset. *See id.* § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note). Section 203(b) (relating to sharing information obtained in intercepting wire, oral or electronic communications under 18 U.S.C.A. § 2517) and (d) (allowing foreign intelligence or counterintelligence and foreign intelligence information obtained in a criminal investigation to be shared with federal law enforcement, immigration, intelligence, national defense, or national security officers) sunset on December 31, 2005. *See id*. In a federal appropriations bill signed into law on December 13, 2003, various pilot projects are authorized to be conducted by the Secretary of Homeland Security to provide training on sharing information on "potential terrorist threats" among local, state and federal officials and private entities with responsibility for managing first responders, counter-terrorist activities, and "critical infrastructure" (Intelligence Authorization Act for Fiscal Year 2004, Pub. L. No. 108-177, § 316, 117 Stat. 2599, 2610–11 (2003)), and by the Director of the Central Intelligence Agency and Secretary of Defense to "assess the feasibility and advisability of allowing intelligence agencies to share and jointly evaluate their respective information." *Id.* § 317, 117 Stat. at 2611–13 (not codified, but published as 50 U.S.C.A. § 403-3 note (West Supp. 2003).

2005,[374] permits information relating to foreign intelligence or counterintelligence or foreign intelligence information[375] that is part of a federal grand jury's records to be disclosed, without any court authorization, to any federal law enforcement, intelligence, immigration, national defense, or national security official for official purposes.[376] Within a "reasonable time after" such disclosure, a government attorney must provide a sealed notice to the court as to the existence and the recipients of the disclosure.[377]

Under a provision of the USA PATRIOT Act that sunsets on December 31, 2005,[378] law enforcement and investigative officers and attorneys for the government[379] may disclose the "contents of any wire, oral, or electronic communication, or evidence derived therefrom" that they lawfully obtain under Title III, to any other federal law enforcement, intelligence, immigration, national defense, or national security official "to the extent that such [information] include[s] foreign intelligence or counterintelligence . . . or foreign intelligence information" for official purposes.[380] Foreign intelligence and counterintelligence information does not have to concern a crime or a foreign person. It may relate to the ability of the United States to defend against a foreign government's hostility

374. *See* USA PATRIOT Act § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

375. *Id.* § 203(d), 115 Stat. at 281 (codified at 50 U.S.C.A. § 403-5d (2003 & West Supp. 2003)). "Foreign intelligence" and "counterintelligence" are defined in the National Security Act of 1947, codified as amended at 50 U.S.C.A. § 401a (2003 & West Supp. 2003) (defining "foreign intelligence" to mean "information relating to the capabilities , intentions, or activities of foreign governments . . . foreign organizations, or foreign persons, or international terrorist activities" and defining "counterintelligence" as "information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments . . . foreign organizations, or foreign persons, or international terrorist activities"), and "foreign intelligence information" is defined in FED. R. CRIM P. 6(e)(3)(D)(iii) as amended by the USA PATRIOT Act § 203(a)(1), 115 Stat. at 279 (defining "foreign intelligence information" to mean "information, whether or not concerning a United States person, that relates to the ability of the United States to protect against . . . actual or potential attack or . . . grave hostile acts . . . sabotage or international terrorism . . . [or] clandestine intelligence activities [by a foreign power or agent of a foreign power, and information] that relates to . . . national defense or the security of the United States [or] . . . conduct of the foreign affairs of the United States")

376. USA PATRIOT Act § 203(a), 115 Stat. at 278–79 (amending FED. R. CRIM. P. 6(e)(3)(D) to authorize such sharing of grand jury information relating to foreign intelligence).

377. *Id.*

378. *Id.* § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

379. I.e., the U.S. Attorney General or authorized assistant, any U.S. Attorney or authorized assistant, and "any other [federal] attorney authorized by law to conduct proceedings under [the Federal Rules of Criminal Procedure] as a prosecutor." FED. R. CRIM. P. 1(b)(1).

380. USA PATRIOT Act § 203(b), 115 Stat. at 280 (amending 18 U.S.C. § 2517 by adding a new clause (6) to authorize the sharing of this information (as foreign intelligence and counterintelligence are defined in The National Security Act of 1947, as amended, in 50 U.S.C.A. § 401a, and as foreign intelligence information is defined as amended in 18 U.S.C.A. § 2510(19) (2000 & West Supp. 2003), which is amended by Section 203(b) of the USA PATRIOT Act, to add a new definition of "foreign intelligence information," conforming such definition with the definition of this term in the FED. R. CRIM. P. 6(e)(3)(D)(iii), as amended by the USA PATRIOT Act § 203(a)(1), 115 Stat. at 278–79. *See also supra* note 373.

or sabotage or international terrorism by a foreign government or entity or a person acting as an agent of a foreign government or entity, or clandestine intelligence activities of such foreign government, entity, or agent, or may relate to our country's national defense or ability to conduct foreign affairs.[381]

6. Foreign Intelligence Surveillance Act of 1978 ("FISA")[382]

The USA PATRIOT Act amends a number of provisions of FISA, which creates a special court that operates in considerable secrecy to grant four categories of orders and warrants. These provisions generally relate to federal officers' ability to obtain information about foreign powers and agents of foreign powers, including in some circumstances United States persons, for the conduct of foreign intelligence or counter-intelligence activities of the United States as well as to protect against international terrorism.[383] In a provision of the USA PATRIOT

381. USA PATRIOT Act § 203(b)(2), 115 Stat. at 280 (amending 18 U.S.C. § 2510(19)). *See* Doyle, *supra* note 10, at 19–23.

382. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C.A. §§ 1801–1862 (2003 & West Supp. 2003)) [hereinafter FISA].

383. *See* 50 U.S.C.A. §§ 1801–1811 (2003 & West Supp. 2003) (FISA electronic surveillance, which the FISA court has jurisdiction to authorize); §§ 1821–1829 (2003 & West Supp. 2003) (FISA physical searches, which the FISA court has jurisdiction to authorize); §§ 1841–1846 (2003 & West Supp. 2003) (use of FISA pen registers and trap and trace devices, as defined in 18 U.S.C.A. 3127 (2000 & West Supp. 2003), which the FISA court, or a federal magistrate designated by the Chief Justice of the United States to act on behalf of a FISA court judge for this purpose, have jurisdiction to authorize); §§ 1861–1863 (2003) (providing access to any tangible things, including business records, which the FISA court, or a federal magistrate designated by the Chief Justice of the United States to act on behalf of a FISA court judge for this purpose, have jurisdiction to authorize).

Id. § 1801(a) (2003) defines "foreign power" as a foreign government, any "entity that is openly acknowledged by a foreign government . . . to be directed and controlled by such foreign government," any "group engaged in international terrorism," any "foreign-based political organization, not substantially composed of United States persons," and any "entity. . . directed and controlled by a foreign government . . . ." "Agent of a foreign power" is defined under 50 U.S.C.A. § 1801(b) (2003) as: (1) anyone who is not a United States person and: either is an officer, employee or member of a foreign power, acting in the United States on behalf of a foreign power or, acts on behalf of a foreign power undertaking clandestine intelligence activities against the United States and (2) anyone, whether or not a United States person, who knowingly: (A) engages in clandestine intelligence gathering involving activities that involve or "may" involve a violation of a U.S. criminal law on behalf of a foreign power, (B) engages in other clandestine intelligence activities that are or are about to violate US criminal laws, (C) engages in sabotage or international terrorism on behalf of a foreign power, (D) enters the United States with a false identity on behalf of a foreign power, or (E) "aids or abets" someone else to do any of these things. *See* Doyle, *supra* note 10, at 12. FISA defines "United States person" as a U.S. citizen, a lawful permanent resident, or entities incorporated or otherwise organized in the United States. *Id*. § 1801(i) (2003). FISA defines "international terrorism" as violent actions that violate US criminal laws (or would if they occurred in the jurisdiction of the United States) that "appear to be intended . . . to intimidate or coerce . . . civilian[s] . . . influence the policy of a government by intimidation or coercion or . . . affect the conduct of a government by assassination or kidnapping," and either "occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale [in which] their perpetrators operate or seek asylum." *Id.* § 1801(c)

Act that does not sunset, Congress provides for an increase in the capacity of the FISA court to issue orders and warrants by increasing the number of FISA court judges from seven to eleven.[384]

The first category of FISA court orders concerns "electronic surveillance," meaning the (i) acquisition of the contents of wire (telephone and voicemail) or radio communications by a United States person in the United States, (ii) acquisition of contents of wire communications to or from any person in the United States (other than computer trespassers), (iii) acquisition of contents of radio communications of any person "if both the sender and all intended recipients are . . . within the United States," or (iv) acquisition of any other information (not wire or radio communications).[385] The second category concerns physical searches. The USA PATRIOT Act's most significant amendment to FISA

(2003). International terrorism may be undertaken by anyone, including a United States person. "Foreign intelligence information" is defined by FISA as (1) "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against . . . actual or potential attack or . . . grave hostile acts . . . [or] sabotage or international terrorism . . . or clandestine intelligence activities" by or of a foreign power or an agent of a foreign power; or (2) "information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to . . . national defense or the security of the United States . . . [or] the conduct of the foreign affairs of the United States." *Id*. § 1801(e) (2003).

The FISA court operates under considerable secrecy and the applications made to the court, records of its proceedings, and orders issued are protected under security measures established by the Chief Justice of the United States in consultation with the Attorney General and the Central Intelligence Agency. *Id.* § 1803(c) (2003). The USA PATRIOT Act § 215, 115 Stat. at 288 (amending 50 U.S.C. § 1862), however, requires the Attorney General to report to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate semi-annually concerning all requests concerning the production of tangible things, and to report to the Judiciary Committees of the House and Senate semi-annually on the number of requests made to, and the number of orders issued by, the FISA Court for the seizure of tangible things. Section 215 sunsets on December 31, 2005. *See id.* § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note). FISA continues to require similar reporting to Congress in connection with electronic, radio and wire surveillance. 50 U.S.C.A. § 1807 (2003) (annual report to U.S. Court's Administrative Office and to Congress on number of applications made and orders and extensions granted); § 1808 (2003) (semi-annual report to Intelligence Committees of House and Senate on all FISA surveillance and use of information obtained in FISA surveillance in criminal cases); § 1826 (2003) (semi-annual report to Intelligence Committees of House and Senate on all FISA physical searches and the number of requests made and orders and extensions granted, as well as on the number of searches involving United States persons' residences, offices or personalty, among other matters); § 1846(2003) (semi-annual report to Intelligence Committees of House and Senate concerning all uses of FISA pen registers and trap and trace devices and number of orders and extensions requested and granted).

384. USA PATRIOT Act § 208, 115 Stat. at 283 (amending 50 U.S.C. § 1803(a) (providing for the Chief Justice of the United States to appoint eleven judges to the FISA court, with three to reside within twenty miles of the District of Columbia)). Section 208 does not sunset. *See id.* § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note). *See also* 147 CONG. REC. S10,547-01, S10,557 (daily ed. Oct. 11, 2001) (statement of Sen. Leahy).

385. 50 U.S.C.A. § 1801(f) (2003). The definition of electronic surveillance referred to in the above text in (i), (iii) and (iv) excludes activities that would not require a warrant for law enforcement activities.

concerns the expansion of the purpose for which a FISA court order may be obtained to allow electronic surveillance and physical searches, and the relaxing of requirements relating to identifying the subject of the order. A provision of the USA PATRIOT Act that sunsets on December 31, 2005,[386] amends FISA to provide that seeking foreign intelligence information (which may include information about United States persons, as provided and limited by FISA) must be a "significant purpose" of an investigation in which a FISA court order for electronic surveillance or a physical search is issued. Foreign intelligence need no longer be the only purpose or a purpose that is so predominant it is virtually the only purpose, as had previously been the case.[387]

This amendment provides access to the FISA process, as an alternative to the Title III process, for criminal investigations as long as gathering foreign intelligence information is a "significant purpose." The FISA process is largely overseen by the Attorney General albeit with detailed applications to the FISA court and reports to Congress, whereas the Title III process involves very significant oversight by the federal court. Title III orders must relate to specified federal crimes for telephone (wire) communications. If the government is seeking foreign intelligence information, it may also access information relating to any federal crime through a FISA order. As other courts are permitted to do in connection with pen registers and trap and trace devices, a provision of the USA PATRIOT Act that sunsets on December 31, 2005,[388] allows the FISA court to issue an order for electronic surveillance that does not specify the person that is subject to the order, but provides for federal law enforcement to enlist from any person assistance, information, and facilities to execute the order "in such a manner as will protect its secrecy," when the target of the surveillance may be taking actions that "may have the effect of thwarting the identification of a specified person" as the subject of the order.[389]

To undertake electronic surveillance or a physical search under FISA, a federal official must apply under oath in writing to the FISA Court for an *ex parte* surveillance order or search warrant authorizing seizure of the contents of electronic, radio, and wire communications or a physical search in connection with obtaining foreign intelligence information.[390] The application must include a certification from a federal official designated by the President that the information

386. *See* USA PATRIOT Act § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

387. *Id.* § 218, 115 Stat. at 291 (amending 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) to provide that a "significant purpose" of a FISA electronic surveillance or physical search must be acquiring foreign intelligence information). *See* Doyle, *supra* note 10, at 9–10. *See also* 50 U.S.C.A. § 1801(e) (2003) (definition of foreign intelligence information).

388. *See* USA PATRIOT Act § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

389. USA PATRIOT Act § 206, 115 Stat. at 282 (amending 50 U.S.C. § 1805(c)(2)(B) to provide for "roving surveillance authority"). *See supra* Part V.3 and note 366.

390. There are limited circumstances, not involving communications, information, premises, or property of a United States person, in which the Attorney General may authorize surveillance or physical searches for up to one year to obtain foreign intelligence information without a court order. *See* 50 U.S.C.A. §§ 1802, 1822 (2003).

sought is foreign intelligence information, stating that a "significant purpose" of the surveillance or search is to obtain foreign intelligence information, stating that the information "cannot reasonably be obtained by normal investigative techniques," and containing the other certifications required by the statute. The Attorney General or the Deputy Attorney General must determine that the application satisfies the requirements of FISA and, on that basis, must approve each FISA order or warrant application before it is submitted to the court. Before being able to approve such applications, the Attorney General must be authorized by the President to do so. Based on the facts and certifications contained in the application and the Attorney General's approval, the FISA court may issue the order or warrant on a finding of probable cause to believe that the target of the electronic, radio, or wire surveillance or the physical search is a foreign power or an agent of a foreign power and the facilities or places where the surveillance is directed or the facilities or premises where the physical search will be undertaken are used, owned, or in the case of physical searches, possessed, by a foreign power or agent of a foreign power.[391] In making its findings to issue a surveillance order or physical search warrant, the FISA court must determine that the facts in the application demonstrate that any United States person (whether an individual or an entity) is not considered to be a foreign power or agent of a foreign power based only on the exercise of his or her rights under the First Amendment to the Constitution.[392]

Provisions of the USA PATRIOT Act that sunset on December 31, 2005,[393] reduce some of the burden on execution of FISA orders for electronic surveillance and physical searches by extending the maximum effective periods of the orders. The maximum duration of a FISA order for electronic surveillance, subject to its further extension through the same process as applies to the order's initial issuance, is generally ninety days and is one year for surveillance of a foreign power that is a foreign government or entity directed or controlled by a foreign government.[394] The USA PATRIOT Act extends the previously applicable ninety-

391. 50 U.S.C.A. §§ 1804, 1805(a)–(b) (2003 & West Supp. 2003) (application for and issuance of orders for electronic, radio and wire surveillance); §§ 1823, 1824(a)–(b) (2003 & West Supp. 2003) (application for and issuance of orders for physical searches); § 1801(g) (2003) (definition of Attorney General to include the Attorney General and the Deputy Attorney General); Exec. Order No. 12,139, 44 Fed. Reg. 30,311 (May 23, 1979) (authorizing electronic surveillance for foreign intelligence purposes as provided in FISA and the Executive Order and authorizing the Attorney General to approve applications and other specified federal officials appointed by the President with confirmation by Congress to provide certifications in support of such applications). *See also* Doyle, *supra* note 10, at 8–19 & nn. 18–43.

392. 50 U.S.C.A. §§ 1805(a)(3)(A), 1824(a)(3)(A) (2003 & West Supp. 2003) (requiring the FISA court in issuing an *ex parte* order approving electronic surveillance or a physical search to find that the facts in the application demonstrate probable cause to conclude that "no United States person [is] . . . considered a foreign power or agent of a foreign power solely upon the basis of activities protected by the first amendment. . . ."). *See* Doyle, *supra* note 10, at 13–14.

393. *See* USA PATRIOT Act § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

394. *Id.* § 207(b)(1), 115 Stat. at 282 (amending 50 U.S.C. § 1805(e)(2) (allowing for extensions of electronic surveillance orders against certain types of foreign powers for up to one year when the FISA court finds that there is probable cause to believe that no communication of a

day period to 120 days for electronic surveillance of an agent of a foreign power (which may include United States persons when specified clandestine intelligence activities for a foreign power, sabotage, or international terrorism activities may involve violation of any U.S. criminal laws).[395] The maximum duration of a FISA order for a physical search, subject to its extension, is extended by the USA PATRIOT Act from ninety days generally and to 120 days for physical searches against an agent of a foreign power.[396] The maximum period, subject to extension, of a FISA order for a physical search against a foreign power that is a foreign government or entity directed or controlled by a foreign government remains one year.[397]

The third and fourth categories of FISA court orders concern pen registers and trap and trace devices and the production of certain items. The USA PATRIOT Act amends FISA to better protect United States persons' First Amendment rights in connection with pen registers and trap and trace devices as well as orders for the production of certain items, while also expanding the reach of such orders. These types of FISA orders had previously been justified when requested to obtain foreign intelligence information and information on international terrorism, which information may include, by definition, information about certain activities of United States persons. Under a provision of the USA PATRIOT Act amendments that sunsets on December 31, 2005,[398] the purpose for which a FISA order for a pen register and trap and trace device or a FISA order for the production of tangible things may be issued, must be to obtain foreign intelligence information "not concerning a United States person" (which restricts the otherwise applicable definition to exclude information on activities of United States persons for this purpose) or to conduct an investigation "to protect against international terrorism or clandestine intelligence activities" (which expands the definition again to include information on certain activities of United States persons), provided that a United States person is not the target of such investigation only based on that person's exercise of First Amendment rights.[399] The overall effect of these

United States person will be acquired, and with the PATRIOT Act amendment, allowing for extensions of such orders against agents of a foreign power for up to one year)).

395. *Id.* § 207(a)(1), 115 Stat. at 282 (amending 50 U.S.C. § 1805(e)(1) by adding a clause (B) (concerning the duration of electronic surveillance)). FISA electronic surveillance orders are generally effective for up to 90 days, except that electronic surveillance against certain types of foreign powers may be for up to one year and surveillance orders against agents of a foreign power may be for up to 120 days. See 50 U.S.C.A. § 1801 (2003) and *supra* note 383 for definitions of "foreign power" and "agent of a foreign power."

396. 50 U.S.C.A. § 1824(d)(2) (2003 & West Supp. 2003) (as amended by USA PATRIOT Act § 207(b)(2), 115 Stat. at 282) (providing for extensions of FISA physical search orders against certain types of foreign powers and agents of foreign powers for up to one year on the court's finding of probable cause to believe that property of United States persons will not be acquired during the extension period).

397. USA PATRIOT Act § 207(a)(2), 115 Stat. at 282 (codified at 50 U.S.C.A. § 1824(d)(1) (2003 & West Supp. 2003)) (concerning the duration of physical searches).

398. *See id.* § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

399. *Id.* § 214(a), 115 Stat. at 286–87; § 505(a), 115 Stat. at 365 (codified at 50 U.S.C.A. § 1842(c)(2) (2003 & West Supp. 2003) and 18 U.S.C.A. § 2709(b) (2000 & West Supp. 2003), respectively) (concerning applications for orders to authorize the use of pen registers and trap and

amendments is to retain an expansive definition of the purpose for which a pen register or trap or trace device or an order for the production of certain items may be obtained, but to ensure that to the extent a United States person is the target, he or she is not the target based only on First Amendment activities. The USA PATRIOT Act amendments greatly expand the reach of a FISA order for the production of items from the previously covered car rental, storage, and hotel records to "any tangible things," including such records and anything else.[400]

To obtain a FISA order for use of a pen register or trap or trace device, the Attorney General, the Deputy Attorney General, or a designated attorney for the federal government must apply under oath in writing to the FISA court or to a U.S. magistrate designated by the Chief Justice of the United States to issue such orders on behalf of a judge of the FISA court.[401] The application must certify that the purposes and targets of the order are as authorized and limited by FISA and identify the federal officer seeking to use the register and device. [402] The court or magistrate will issue an *ex parte* order upon a finding that the application satisfies the statute, and the order will identify the subjects of the investigation and order "if known," will specify the types of communications covered, the location of the lines or facilities to which the register and device will be attached, and the geographic limits of the trap and trace authority, will order electronic communications service providers, landlords, or other persons to provide technical assistance and information and facilities to assist in the execution of the order, and will order those persons or entities not to disclose the investigation unless and until ordered to do so by the court.[403] The executing official is required to compensate any person who provides such assistance.[404]

To obtain a FISA court order for the production of business records and any other tangible thing, the Director of the FBI or her designee (who must be an Assistant Special Agent in Charge or higher FBI official), must apply to the FISA court or to a U.S. magistrate designated by the Chief Justice of the United States to issue such orders on behalf of a judge of the FISA court.[405] The application must

trace devices); Doyle, *supra* note 10, at 16–17, note 51. *See* 50 U.S.C.A. §§ 1801(c), 1841(1) (2003) (defining international terrorism); § 1841(2) (2003) (pen registers and trap and trace devices are defined as in 18 U.S.C.A. § 3127 (2000 & West Supp. 2003)); §§ 1801(e), 1841(1) (2003) (defining foreign intelligence information). *See also* S. REP. NO. 95-604(I), at 22–24 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3922–26 (Senate's section by section analysis of FISA as it was to be enacted, which defines "clandestine intelligence activities" as various activities constituting spying or covert information gathering for a foreign power).

400. USA PATRIOT Act § 215, 115 Stat. at 287–88 (amending 50 U.S.C. § 1861). *See* Doyle, *supra* note 10, at 17–19, note 41. Section 215 sunsets on December 31, 2005. *See* USA PATRIOT Act § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

401. 50 U.S.C.A. § 1842(a)(1) (2003).

402. *Id*. § 1842(c) (2003).

403. *Id*. § 1842(d) (2003).

404. USA PATRIOT Act § 214(a), 115 Stat. at 286 (amending 50 U.S.C. § 1842). There are also emergency provisions that allow the use of pen registers and trap and trace devices on approval and authorization of the Attorney General or Deputy Attorney General, with notice to the FISA court and the filing of an application "as soon as practicable" but no later than forty eight hours after such use. 50 U.S.C.A. § 1843(a)(2) (2003 & West Supp. 2003).

405. 50 U.S.C.A. § 1861(a) (2003).

certify that the records sought are for the purposes authorized by the statute and do not exceed FISA's limitations for such orders. The court or magistrate will issue an *ex parte* order on a finding that the statutory requirements are satisfied.[406]

The USA PATRIOT Act also allows any foreign intelligence or counterintelligence or foreign intelligence information obtained as part of any criminal investigation to be disclosed to federal intelligence, law enforcement, immigration, national defense, and national security officers for official purposes. This provision enhances the sharing of information among the federal law enforcement, intelligence, and national security and defense communities.[407]

VI. EXPORT CONTROLS: KEY PROVISIONS AND ENFORCEMENT INITIATIVES RELATING TO BIOTERRORISM PREVENTION AND HOMELAND SECURITY

Export controls are an area of federal law and regulation that predates by decades September 11, 2001, but is presently regarded by the federal government as a useful tool in its war on terrorism. A complete discussion of the intricate requirements of export controls is beyond the scope of this article.[408] It is, however, important to appreciate export controls' basic regulatory scheme and scope of application because indications are that these laws will be enforced more frequently and with greater focus on the academic sector than has been the case in the past. Export controls apply to many technologies, equipment, chemicals, biological agents and toxins, materials, goods, and software code ("technologies, materials and items") developed or used in biological and other areas of research, and to information, training, and instruction relating to covered technologies,

406. USA PATRIOT Act § 215, 115 Stat. at 287 (codified at 50 U.S.C.A. § 1861 (2003 & West Supp. 2003)). Section 215 sunsets on December 31, 2005. *See id*. § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note).

407. *Id*. § 203(d), 115 Stat. at 281 (codified at 50 U.S.C.A. § 403-5d (2003 & West Supp. 2003)) (providing that this sharing of information may occur "[n]otwithstanding any other provision of law" but "subject to any limitations on the unauthorized disclosure of such information"). This subsection sunsets on December 31, 2005. *Id.* § 224, 115 Stat. at 295 (not codified, but published as 18 U.S.C.A. § 2510 note). Foreign intelligence and counterintelligence are defined in the National Security Act of 1947, codified as amended at 50 U.S.C.A. § 401a (2003 & West Supp. 2003), and foreign intelligence information is defined in Section 203(d) of the USA PATRIOT Act (amending 50 U.S.C. § 1801(e)). These definitions conform with similar definitions in USA PATRIOT Act § 203(a), 115 Stat. at 278-80 (from which is derived FED. R. CRIM. P. 6(e)(3)(D) to permit the sharing of grand jury records relating to these subjects without court authorization); § 203(b), 115 Stat. at 280 (amending 18 U.S.C. § 2517 to allow sharing of the contents of wire, oral or electronic communications lawfully obtained under Title III when the contents include such subjects). *See supra* notes 374 and 378.

408. For additional information on export controls, refer to the U.S. Department of Commerce, Bureau of Industry & Security website at http://www.bis.doc.gov/ (last visited Apr. 4, 2004); the U.S. Department of State, Directorate of Defense Trade Controls website at http://pmdtc.org/ (last visited Mar. 31, 2004); and the U.S. Department of the Treasury, Office of Foreign Assets Control website at http://www.ustreas.gov/offices/eotffc/ofac/ (last visited Apr. 4, 2004). A number of texts provide useful commentary on export controls including COPING WITH U.S. EXPORT CONTROLS (PLI Com. Law & Practice Course, Handbook Series No. A4-4527, 1997).

materials and items.[409] When covered chemicals or biologicals are involved and an exclusion does not apply, the requirements of export controls must be satisfied in addition to the requirements of the BPARA and its regulations and the USA PATRIOT Act. Academic institutions and their researchers can take steps to qualify much of their research and teaching for regulatory exclusions, but they must understand and adhere to the prerequisites for exclusion. Institutions and individuals must obtain export licenses and otherwise comply with export controls when exclusions do not apply and a license is necessary.[410] Violation of export controls can carry criminal and civil penalties against the individual involved as well as the institution.[411]

Export controls are intended to advance the United States' foreign policy goals, to restrict exports of goods, technology, and information that could enhance the military potential of other countries (both adversaries and friendly nations), to prevent the proliferation of nuclear, chemical, and biological weapons of mass destruction, to prevent terrorism, and to perform the United States' obligations under various foreign treaties and agreements with other nations, such as the Nuclear Non-Proliferation Treaty.[412] When export controls apply, they apply to U.S.-origin technologies, materials, and items and related information, training, and instruction, wherever they are located or take place, whether in the United States or abroad.[413] Underlying the export control regime is the principle that it is a privilege and not a right for U.S. citizens and permanent residents (individuals and entities) to "export" covered technologies, materials, and items and related information.[414] Consequently, an academic institution should establish good programs of export control education and compliance for the benefit of the

409. *See* Commerce Control List, *infra* note 421, and U.S. Munitions List, *infra* note 427.

410. *See* 15 C.F.R. § 764.3 (2004) (providing civil and criminal penalties for willful violation of the Commerce Department's EAR); 22 C.F.R. § 123.1 (2000) (requirement for export or temporary import licenses).

411. Criminal penalties for willful violations under the Commerce Department's EAR are up to $250,000 and/or up to ten years imprisonment for each violation for individuals, and up to the greater of $1,000,000 or five times the value of the export for entities, depending on when the violation occurred. 15 C.F.R. § 764.3(b). Civil fines are from $10,000 to $100,000 per violation depending on when the violation occurred and the classification of the goods or technology involved. The Commerce Department can assess multiple violations per shipment. *Id.* § 764.3(a). Criminal penalties assessed against individuals and entities for willful violation of the State Department's ITAR are up to $1,000,000 and/or up to ten years imprisonment for each violation. 22 U.S.C. § 2778(c) (2000). Civil fines are up to $500,000 per violation. *Id.* § 2778(e). Criminal penalties for violation of OFAC's regulations are up to $1,000,000 in fines for entities and $250,000 in fines for individuals, along with the potential for up to ten years of imprisonment. 31 C.F.R. § 515.701 (2003). Civil fines are up to $55,000 per violation. *Id.*

412. *See*, *e.g.,* 15 C.F.R. § 730.6 (national security, foreign policy, nonproliferation and terrorism); 15 C.F.R. § 742.3(b)(viii)(A) (Nuclear Non-Proliferation Treaty).

413. For example, the State Department regulates the sending or taking of a defense article out of the United States or disclosing technical data to a foreign person whether in the United States or abroad. 22 C.F.R. § 120.17(1), (4). The Commerce Department regulates actual shipments out of the U.S. as well as a release of technology or source code subject to the controls in a foreign country, or to a foreign national in the United States. 15 C.F.R. § 734.2(b)(1)–(2).

414. 15 C.F.R. § 764.3(a)(2).

institution and its researchers.

There are two major export control regulatory schemes.[415] The Export Administration Regulations ("EAR"),[416] implementing the Export Administration Act of 1979, as amended,[417] among other federal authorizations,[418] are administered by the Bureau of Industry and Security ("BIS") of the Commerce Department under the Secretary for Industry and Security. The EAR generally governs "exports,"[419] of technology, materials, and items that may have a "dual use," meaning that they are largely commercial but may have both commercial and military applications, as well as information concerning such items.[420] The EAR lists the items subject to its regulation on the Commerce Control List ("CCL"), which includes a "catch-all" category, EAR 99.[421]

The International Traffic in Arms Regulations ("ITAR"),[422] implementing the Arms Export Control Act among other federal authorizations,[423] are administered by the Directorate of Defense Trade Controls ("DDTC") of the State Department, under the Under Secretary for International Security and the Assistant Secretary for Political-Military Affairs.[424] The ITAR generally governs "exports"[425] of defense articles (including certain technologies, materials, and items and related "technical data" and "defense services" (information, training, and instruction)) (a) that are "specifically designed, developed, configured, adapted, or modified for a military application . . . [do] not have a predominant civil application[], and . . . [do] not have [a] performance equivalent . . . to those of an article or service used for civil applications" or (b) that are "specifically designed, developed, configured, adapted, or modified for a military application, and [have] a significant military or intelligence applicability."[426] Many regulated defense articles are listed on the

415. The Nuclear Regulatory Commission's ("NRC") regulations, 10 C.F.R. § 110 (2004), under the Atomic Energy Act of 1954, codified as amended at 42 U.S.C. §§ 2011–2097 (2000), govern the export of nuclear reactor vessels and related materials and technology. The Department of Energy's regulations, 10 C.F.R. § 810.1 (2004), under the Atomic Energy Act of 1954, govern the export of technology concerning special nuclear materials. The United States Patent and Trademark Office's regulations, 37 C.F.R. § 5.1 (2003), govern export of "unclassified technology in the form of a patent application or an amendment, modification, or supplement thereto." To the extent regulated by these other authorities, technologies, materials, and items, and related information, are not subject to the EAR or ITAR. *See* 15 C.F.R. §§ 734.3(b)(iii)–(v) (2004); 22 C.F.R. §§ 123.20, 120.10, 120.11(5).

416. 15 C.F.R. §§ 730–774.

417. 50 U.S.C.A. §§ 2401–2420 (2003 & West Supp. 2003). The Export Administration Act has lapsed. Its provisions are being implemented through Executive Order. *See infra* note 418.

418. *E.g.,* Executive Orders under the International Emergency Economic Powers Act, *id.* §§ 1701–1706 (2003).

419. 15 C.F.R. § 734.2(b).

420. *Id*. §§ 730.1–730.3, 730.5–730.7, 734.

421. *See id*. § 774 [hereinafter Commerce Control List].

422. 22 C.F.R. §§ 120–130.

423. 22 U.S.C.A. § 2778 (1990 & West Supp. 2003).

424. 22 C.F.R. § 120.1.

425. *See id*. § 120.17, 120.19 ("export" and "reexport," respectively).

426. *Id.* § 120.3(a)–(b). *See also id.* § 120.6 ("defense article"), § 120.9 ("defense service"), 120.10 ("technical data").

United States Munitions List ("USML"),[427] although this list is not as specific as the CCL under the EAR, and ITAR regulation relies as well on general standards. ITAR regulates technologies, materials, and items that are designed to kill or injure in a military context, as well as technologies and items that are designed to defend against such death and injury.[428] Seemingly innocuous equipment, such as mini research submersibles (even if not intended by the creator for a military application),[429] can be included on the USML depending on their configuration. Articles or services that in the State Department's judgment are specifically designed, developed, configured, adapted, or modified for a military application and do not have predominant civil applications, as well as those articles and services with significant military or intelligence application that, in the State Department's judgment, require control, fall under the ITAR.[430] In addition to regulating USML-listed defense articles and related defense services, ITAR regulates other technologies, materials, and items (and related information, training and instruction), when there is reason to know that they will be used in or for weapons of mass destruction or when they are designed or modified for military use.[431]

Supplementing these two export controls regulatory schemes are the regulations of the Office of Foreign Assets Control ("OFAC") of the U.S. Treasury Department. The OFAC regulations govern transactions with and transfers or travel to certain foreign countries, and transactions with and transfers to certain end-users who are deemed to be involved in terrorism, the drug trade, or other illicit activities.[432] These regulations implement United States' trade embargoes and economic sanctions against specified countries, entities, and individuals.[433]

Of particular note for colleges and universities in the post-September 11 world, is the fact that there are many biological materials and chemicals, as well as equipment that may be used to distribute or work with them, that are on the CCL or USML or are otherwise covered by the EAR and ITAR.[434] Most select biological agents and toxins that are subject to the USA PATRIOT Act and BPARA and its regulations are also subject to the EAR and ITAR.[435] Appendices

427. *Id*. § 121.1 [hereinafter U.S. Munitions List].

428. *See id*. .

429. *See id.* § 121.15 (vessels of war and special naval equipment, including all submarines designed, modified or equipped for military purposes).

430. *Id.* §§ 121.1, 120.3(b).

431. *See id.* § 120.3 (policy on designating and determining defense articles and services, including those that are specifically designed, developed, configured, adapted or modified for a military application, which do not have predominant civil applications as well as those with significant military or intelligence applicability); *id.* § 121.1, at Category XVI: Nuclear Weapons, Design and Testing-Related Items.

432. *See* 31 C.F.R. § 500 (2003).

433. *Id.*

434. Included on the USML are certain toxicological agents and equipment and radiological equipment. *See* 22 C.F.R. § 121.1, at Category XIV. The CCL also contains biological materials and chemicals. *See, e.g.,* 15 C.F.R. pt. 774 (2004), Supp. 1, at 1C 350–355.

435. *See* 22 C.F.R. § 120 (ITAR) and 15 C.F.R. §§ 730–774 (2004) (EAR).

G, H, and I[436] of this article contain a chart generally outlining the basic regime of export controls under the EAR and ITAR and certain of their exclusions, a chart generally outlining the regulation of biological materials and chemicals under the EAR and ITAR, and a listing of countries that are relevant to the application of export controls and OFAC embargoes.

As a general matter, an "export" under the EAR and ITAR is the transfer outside of the United States of any regulated technologies, materials, or items, including equipment, software source and object code, goods, chemicals, biologicals, and other materials (i.e., those on the CCL or USML or otherwise covered by the regulations) or the disclosure abroad of any related information, training, instruction, or technical data concerning controlled technologies, materials or items (information and data beyond general and basic marketing information), transmitted in any medium (whether oral, visual, via computer or other electronic, wire, or radio transmission, or physical).[437] "Export" also includes transfer of ownership or control of such technologies, materials, and items.[438] It does not matter for purposes of defining "export" whether the recipient abroad is a U.S. citizen or lawful permanent resident or is a foreign national, although mere travel abroad by an individual whose personal knowledge includes regulated technologies, materials, and items is not an "export."[439]

A "deemed export" is the transfer or disclosure of information, training, instruction, or technical data (but not the mere transfer of the technologies, materials, or items, without any related information, training, instruction, or technical data) to a foreign national in the United States.[440] Campuses are rife with opportunities for deemed exports because many campuses' student bodies, faculties, and visitors are international.

Unless an exclusion from regulation applies, before any export or deemed export (even on campus) of technologies, materials, and items (or related technical data, information, training, or instruction) regulated under the ITAR may occur, and before some such exports or deemed exports regulated under the EAR may occur, a license must be obtained from the relevant agency, DDTC or BIS.[441] This

436. For Appendix G, Expert Controls and Embargoes Key, visit The Journal of College and University Law, Symposium Webpage, *at* http://www.nd.edu/~jcul/USA_PATRIOT_Act/Appendix_G.pdf (last visited Apr. 4, 2004). For Appendix H, Export Controls of Chemicals/Bio-Agents/Toxins, visit The Journal of College and University Law, Symposium Webpage, *at* http://www.nd.edu/~jcul/USA_PATRIOT_Act/Appendix_H.pdf (last visited Apr. 4, 2004). For Appendix I, Export Controls and Embargoes Table, visit The Journal of College and University Law, Symposium Webpage, *at* http://www.nd.edu/~jcul/USA_PATRIOT_Act/Appendix_I.pdf (last visited Apr. 4, 2004).

437. *See* 15 C.F.R. § 734.2.

438. *Id.*

439. *See* 22 C.F.R. § 120.17 ("export"), 120.19 ("reexport"), § 120.10 ("technical data"), 120.9 ("defense service"); 15 C.F.R. § 734.2(b). Note that traveling abroad with a computer on which EAR or ITAR-regulated encrypted software code is loaded may be an export. *See* 15 C.F.R. § 734.2.

440. *See* 15 C.F.R. § 734.2; 22 C.F.R. § 120.17.

441. The State Department regulates the sending or taking of a defense article out of the U.S. or disclosing technical data to a foreign person whether in the U.S. or abroad. 22 C.F.R. §

means that before a faculty member may send controlled technologies, materials, or items to a United States or foreign colleague in a foreign country, or may collaborate with or train a United States or foreign colleague abroad or a foreign colleague in the United States concerning such items, a license must be obtained if an exclusion from regulation does not apply and a license is required. Obtaining a license can take a few months to half a year or, in some cases, longer. Licenses may be required for exports to "friendly" foreign locales and nationals, such as those in Canada, countries in Europe and Australia, as well as for exports to more unfriendly foreign locales and nationals.[442] If an exclusion from regulation does not apply and a license is required but denied, the export abroad or deemed export in the United States (even on campus) may not occur and the faculty member cannot pursue his or her plans.[443]

An ITAR license will be required, and likely will be denied (meaning that the export will be prohibited), if the proposed export of an ITAR regulated defense article (including USML-listed and otherwise regulated technologies, materials, and items) or related defense service (technical data, training, or instruction) is to an ITAR prohibited country or a United Nations Security Council arms embargoed country.[444] Otherwise, a license will be considered and granted or denied on a case-by-case basis.[445]

An EAR license may be required for a proposed export of technologies, materials, and items (or related information, training, and instruction) listed on the CCL under the catch-all EAR 99 category, if the export involves an entity or person on the EAR entity list or denied person list, a prohibited end-use such as a weapons of mass destruction program, an OFAC embargoed country, any other U.S. embargoed country, or anyone listed on the OFAC prohibited list.[446] Otherwise no license will be required for EAR 99 listings.[447] An EAR license may be required, and will be considered and granted or denied on a case-by-case basis, if the proposed export concerns CCL-listed technologies, materials, or items in CCL categories other than EAR 99, depending on the destination and end user.[448] Licenses may be required under the EAR for exports to certain entities or individuals in a country, even when exports to other entities or individuals in the same country do not require a license.[449]

120.17(1), (4). The Commerce Department regulates actual shipments out of the U.S. as well as a release of technology or source code subject to the controls to in a foreign country, or to a foreign national in the United States. 15 C.F.R. § 734.2(b)(1)–(2)(2004).

442. *See* Country Control Chart, 15 C.F.R. § 738, Supp. 1 (2004).

443. *See supra* note 441 and accompanying text.

444. 22 C.F.R. § 126.1. See Appendices G and I, *supra* note 436, for a current listing (subject to change) of such countries.

445. 22 C.F.R. § 120.20.

446. 15 C.F.R. § 732.3.

447. *See, e.g.,* 15 C.F.R. § 732.3(d)(5) and following General Prohibitions. See also Appendices G and I, *supra* note 436, for a current listing (subject to change) of such countries.

448. 15 C.F.R. § 732.1.

449. *See, e.g.,* Entity List, 15 C.F.R. § 744, Supp. 4; Denied Person List, 15 C.F.R. § 764 Supp. 2 (updated at http://www.bis.doc.gov/DPL/Default.shtm (last visited Apr. 4, 2004)).

An EAR license is required for the export of chemicals or biological agents or toxins listed on the CCL for chemical and biological weapons control ("CB") purposes to any country (even Canada). Such license will be denied (meaning the export will be prohibited) if the proposed export is to Syria or an OFAC or other U.S. embargoed country or to an end user who is on the EAR denied person list. Otherwise a license will be considered on a case-by-case basis.[450] An EAR license will be required and likely will be denied (meaning the export will be prohibited) for exports of chemicals or biological agents or toxins listed on the CCL for chemical weapons convention compliance ("CWC") purposes, including for Ricin D and E and Saxitoxin, to any country that is not a party to the Chemical Weapons Convention.[451]

When an EAR or ITAR license is not required for controlled technologies, materials, or items, and when an export is exempt from licensing, export documentation is still required.[452] Even if an exclusion from export controls applies, as discussed below, there may still be restrictions on travel to or transactions and transfers with certain embargoed locales or individuals under the OFAC regulations.[453]

Many technologies, materials, and items used or developed in academic research settings are on the CCL or USML or are otherwise regulated by EAR or ITAR. A very small percentage of academic research activities, however, should be subject to control or licensing because many such activities can qualify for the "fundamental research," the "public domain"/"publicly available," or certain other exclusions from EAR and ITAR regulation, or for exemptions from their licensing requirements.

The "public domain" exclusion under ITAR[454] and the "publicly available" exclusion under EAR[455] are the broadest available exclusions from export controls. These exclusions, if they apply, allow deemed exports in the United States and exports abroad without export controls applying at all, even if the export involves a prohibited, embargoed, or restricted country. These exclusions expressly apply only to the export or deemed export of information, not to the export of USML or CCL-listed or otherwise controlled technologies, materials, items (such as covered equipment, encrypted software, chemicals, or biological agents or toxins), or

450. *See* 15 C.F.R. pt. 738, Supp. 1; 15 C.F.R. § 774, Supp. 1, at 1C 351-54.

451. *See* 15 C.F.R. § 742.18 (license required for export to non-Chemical Weapons Convention country, unless an end user certificate is issued by the governments of all importing countries). If an item or technology is listed for chemical weapons convention compliance purposes as well as chemical and biological weapons control and/or anti-terrorism purposes, the license requirements for all such listing purposes apply. 15 C.F.R. § 774, Supp. 1, at 1C 355 (regarding chemical weapons convention compliance), 1C 350 (regarding precursors for toxic chemicals); 15 C.F.R. pt. 738, Supp. 1 at 1C 355 (regarding weapons control and anti-terrorism). See Appendix G, *supra* note 436, for a current listing of Chemical Weapons Convention countries (subject to change).

452. 22 C.F.R. § 123.6 (2003); 15 C.F.R. § 740.1(f).

453. For a summary of various sanctions programs at the OFAC website, see http://www.ustreas.gov/offices/eotffc/ofac/ (last visited Apr. 4, 2004).

454. 22 C.F.R. §§ 120.10–120.11.

455. 15 C.F.R. §§ 734.3(b)(3), 734.7.

services. To qualify for these exclusions, there must not be a reason to believe that the exported information will be used in or for weapons of mass destruction. In addition, the federal government must not have imposed export controls or restrictions as a funding condition. It is critical that neither the institution, nor the principal investigator, agrees to restrict public disclosure, to limit participation by foreign nationals, or to accept any other export controls as a condition to funding, or the information will not qualify for these public domain and public availability exclusions.[456]

Information, including non-encrypted software code, that is already published (not just ordinarily published), through or at one or more of the following means or outlets are in the "public domain" or are "publicly available," and consequently are not subject to export controls: a) libraries open to the public, including most university libraries; b) unrestricted subscriptions, newsstands, and/or bookstores for a price not exceeding reproduction and distribution costs plus a reasonable profit; c) U.S. patents and open (published) patent applications; d) conferences, meetings, seminars, trade shows, and exhibitions held in the United States, which are generally open to the public for a fee reasonably related to the cost, and at which attendees may take notes and from which attendees may leave with their notes; and e) web sites that are accessible to the public, free of charge, and without the host's knowledge or control of who visits or downloads software or information.[457] If only EAR information and non-encrypted software are involved (and ITAR is definitely not implicated), the information and software may be published through or at such conferences, meeting, seminars, trade shows, and exhibitions, wherever held (in the United States or abroad).[458]

A closely related exclusion under ITAR concerns information (not technologies, materials, and items such as equipment, chemicals, biological agents or toxins, or encrypted software), that constitutes "general scientific, mathematical or engineering principles commonly taught in schools, colleges, and universities."[459] This ITAR exclusion is useful for certain commonly taught information, but not for other information. A closely related exclusion under EAR concerns "educational information," meaning information "released by instruction in catalog courses and associated teaching laboratories of academic institutions" wherever

456. The acceptance of any of these restrictions also will result in the invalidation of the fundamental research exclusion under the ITAR at 22 C.F.R. § 120.11(8) and the EAR at 15 C.F.R. § 734.8, although, under the EAR, the acceptance of national security controls in government sponsored research that is solely subject to the EAR may qualify for an exclusion under 15 C.F.R. § 734.11.

457. Information in the "public domain" and "publicly available" is outlined in the ITAR under 22 C.F.R. § 120.11 and § 120.10(5). Information in the "public domain" and "publicly available" is outlined in the EAR under 15 C.F.R. § 734.3(b)(3) and §§ 734.7–734.9. Information on export controls on patent applications can be found at 22 C.F.R. § 125.2(b) and 15 C.F.R. § 734.10 (EAR), as well as 37 C.F.R. § 5 (Secrecy of Certain Inventions and Licenses to Export and File Applications in Foreign Countries). Web sites are clearly an authorized means of publication under EAR and are probably an acceptable means of publication under ITAR, although there is no formal guidance on this point from the Department of State.

458. 15 C.F.R. §§ 734.3(b)(3), 734.7.

459. 22 C.F.R. § 120.10(5).

such institutions are located (in the United States or abroad).[460] This EAR exclusion is useful in classroom and teaching laboratory settings, but not in other lectures, research laboratories, or impromptu conversations that are not associated with a course listed in the institution's course catalogue.

ITAR exempts from its licensing requirements disclosures by "U.S. institutions of higher learning" in the United States of unclassified technical data to foreign national "bona fide and fulltime regular employees" of these institutions who are not nationals of ITAR-prohibited or embargoed countries.[461] The college or university must inform any such employee in writing that the disclosed technical data "may not be transferred to other foreign persons" without "prior written approval of the Office of Defense Trade Controls."[462] This exclusion does not apply to students employed part-time and holding F-1 visas or to other holders of types of visas that do not permit full-time employment.

Perhaps the most well-known exclusion from export controls that is commonly relied upon by academic institutions is the U.S. university fundamental research exclusion under the EAR and the ITAR.[463] This exclusion is founded on the principles of National Security Decision Directive 189 of 1985 ("NSDD 189"), which provides that classification is the appropriate means for securing information related to "fundamental research" by colleges and universities. "Fundamental research" is defined under NSDD 189 as "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."[464] It is critical to the openness of U.S. campuses that supports our country's leadership position in both innovation in fundamental research and, ultimately, innovation and economic competitiveness in the marketplace, that NSDD 189's approach to securing fundamental research when necessary through classification be maintained.[465] It is significant to note that the Reagan Administration, which promulgated NSDD-189 despite its concern about the potential for the Soviet Union and other communist countries to take advantage of U.S. openness, recognized the importance of fundamental research to the strength of our country's national security. The George W. Bush Administration, in November 2001, confirmed that NSDD 189 continues to be the policy of the federal government.[466]

460. 15 C.F.R. §§ 734.3(b)(3)(iii), 734.9.

461. 22 C.F.R. §§ 125.4(b)(10), 126.1. See Appendices G and I, *supra* note 436, for a current listing of such countries (subject to change).

462. *See* 22 C.F.R. §§ 125.4(b)(10).

463. 15 C.F.R. § 734.8(a)–(b); 22 C.F.R. § 120.11(8).

464. NAT'L SEC. DECISION DIRECTIVE 189, NATIONAL POLICY ON THE TRANSFER OF SCIENTIFIC, TECHNICAL AND ENGINEERING INFORMATION (Sept. 21, 1985), *available at* http://www.fas.org/irp/offdocs/nsdd/nsdd189.htm [hereinafter NSDD 189].

465. *See* MIT Ad Hoc Faculty Committee, *supra*, note 4.

466. In a November 1, 2001, letter to Dr. Harold Brown, Co-chairman of the Center for Strategic & International Studies, Dr. Condaleeza Rice, Assistant to the President for National

It is easy to misunderstand the breadth of the fundamental research exclusion. Even NSDD-189, which notes that it is the government's policy not to place restrictions upon the conduct or reporting of federally funded fundamental research that has not received national security classification nevertheless permits restrictions "as provided in applicable U.S. statutes."[467] Many academic institutions assume incorrectly that any activities they undertake are covered by the exclusion merely because they are colleges and universities, eliminating any concern about export controls. This is not a correct assumption.

"Fundamental research" under the EAR is information (including non-encrypted software code, but not any technologies, materials, or items) resulting from "basic and applied research in science and engineering" conducted at an "accredited institution[] of higher education located in the United States" that is "ordinarily published and shared broadly within the scientific community" and that is not "restricted for proprietary reasons or specific national security reasons."[468] ITAR defines "fundamental research" with nearly identical language.[469] ITAR, however, uses the phrase "higher learning," and the restrictions for proprietary reasons phrase reads, "specific U.S. Government access and dissemination controls."[470] To qualify for the fundamental research exclusion or any other exclusion from the EAR or ITAR, there cannot be any reason to know that the information will be used in or for weapons of mass destruction.[471] It is also necessary that the information be "ordinarily published" (but not necessarily actually published) in order for the fundamental research exclusion to apply to college and university research results.[472] The State Department has been less willing to provide guidance on compliance with ITAR and has been stricter in its approach than the Commerce Department has been on compliance with EAR. If an ITAR prohibited country is involved, it is prudent in the current environment (although it is not required under the literal words of the regulations) to take steps

Security Affairs, stated, "the policy on the transfer of scientific, technical, and engineering information set forth in NSDD-189 shall remain in effect, and we will ensure that the policy is followed" while a "broad-based review" ensues of "technology transfer controls." A copy of this letter is available at http://www.aau.edu/research/Rice11.1.01.html (last visited Apr. 4, 2004). A report on the review referred to in the letter has not been publicly released at the time this article went to the printer.

467. NSDD 189, *supra* note 464.

468. *See* 15 C.F.R. § 734.8(a)–(b). The EAR, but not the ITAR, provides a similar exclusion for corporate research that qualifies as "fundamental research" where the researchers are "free to make scientific and technical information resulting from the research publicly available without restriction or delay based on proprietary concerns or specific national security controls." *Id*. § 734.8(d).

469. *See* 22 C.F.R. § 120.11(8) (2003).

470. *Id.*

471. The EAR contains an explicit prohibition on weapons of mass destruction programs at 15 C.F.R. §§ 744.2–744.6. The restrictions in the ITAR are implicit, including not supporting a military application at 22 C.F.R. § 120.3, and through various references in the U.S. Munitions List including Category IV (ballistic missiles), Category XIV (biological and chemical agents), Category XV (spacecraft systems and associated equipment), and Category XVI (nuclear weapons, design and testing related items).

472. *See* 15 C.F.R. § 734.8(a)–(b); 22 C.F.R. § 120.11(8).

to actually publish research results when relying on the fundamental research exclusion.[473]

Publication restrictions may not be applied to research results or the fundamental research exclusion will be destroyed. This is a point worth underscoring. If an institution, or its researcher, agrees to any publication or access restrictions, even in an agreement separate from the funding award or even if required by a government funding agency, the fundamental research exclusion will not apply. Federal agencies have tried to require their review and approval of research results prior to publication, or to impose other restrictions on colleges and universities, as a condition to funding research that the agencies deem to be "sensitive but not classified." These restrictions conflict with the policies underlying NSDD 189; and if a university accepts such restrictions, it is accepting the applicability of export controls because the fundamental research public domain/public availability exclusions will be destroyed.

A short delay in publication only for purposes of allowing sponsor review to ensure that sponsor-provided proprietary information is not inadvertently disclosed or to allow the institution or the sponsor to seek patent protection, is permitted under EAR and may be permitted under ITAR, without destroying the exclusion.[474] Note, however, that the results of the research itself may not be proprietary or the fundamental research exclusion will not apply.[475] And, if a sponsor provides proprietary information to the college or university researcher concerning technologies, materials, or items that are subject to the EAR or ITAR, that sponsor information is subject to export controls, and both the university and the sponsor must comply.[476]

It is critical to appreciate that one cannot create research information or non-encrypted software that qualifies for the fundamental research exclusion anywhere other than at an accredited institution of higher learning located in the United States. Foreigners can participate in fundamental research only in the United States at an accredited college or university. With one very limited exception that applies to certain ITAR-regulated space satellite technology and related information (and that some institutions have concluded is not useful in practice), U.S. university faculty and students cannot do research abroad under the fundamental research exclusion. Once fundamental research is created at an

473. The State Department has occasionally taken the view in its informal guidance that despite the language of "ordinarily published" that is used in the definition of fundamental research in 22 C.F.R. § 120.11(8), the introductory language to § 120.11, which lists a number of "public domain" exclusions including one for "fundamental research," requires information to be "published" to qualify for exclusion. This interpretation is not well supported by the regulatory language most specifically addressing qualification for the fundamental research exclusion. Should the State Department ever seek to test or issue formal guidance on the requirements of this exclusion, it would likely do so in circumstances involving an ITAR-prohibited country. Consequently, it is prudent to take extra precautions in such circumstances.

474. *See* 15 C.F.R. § 734.8(b)(2)–(3). The ITAR does not provide specific guidance on this point.

475. *See* 15 C.F.R. pt. 734, Supp. 1 (2004), at Section D: Research, Correspondence, and Informal Scientific Exchanges, Question D(7) and Answer.

476. *See* 15 C.F.R. § 734.8(b)(4)–(5); 22 C.F.R. § 120.11(8).

accredited college or university in the United States, however, this information (but not CCL or USML listed or otherwise regulated technologies, materials, and items such as equipment, encrypted software, chemicals, or biological agents or toxins) can be exported abroad without export controls applying at all.[477]

The National Defense Authorization Act[478] requires the Commerce Department, the Department of Energy, the Defense Department, and the State Department, in consultation with the Central Intelligence Agency ("CIA") and the FBI, to assess whether U.S. export controls are adequately preventing acquisition by foreign governments, agents of foreign powers and other non-U.S. citizens of sensitive U.S. technology and services on how to use it. These agencies are required to report annually to Congress on their findings. In their 2003 report, the agencies are focusing on whether academic research institutions, with their multi-national campus communities, are well informed about and complying adequately with export controls, including such controls on "deemed exports" to foreign nationals on campus. In the fall of 2003, Inspector General's staff representing the Department of Commerce and the State Department (as well as the Departments of Energy and Defense), visited nine major academic research institutions across the country. The Inspector General of the Department of Defense issued a report to Congress in March 2004 and another report is expected.[479] Any issues will inform on-going government consideration about the wisdom of following NSDD 189. This focus arose after the General Accounting Office criticized the Commerce Department in a 2002 report to Congress for lax enforcement of the EAR in academia, particularly in connection with "deemed exports" to foreign nationals on campus. Congress and the export control, major science funding, and defense agencies are presently questioning and assessing the effectiveness of export controls to stem what they perceive to be a threat that academic institutions could transfer sensitive technology to potential terrorists.

At the same time, the effectiveness of any controls short of classification on the exchange of technology and related information in our global science community, in our Internet age, and in our global economy, is questionable. Rather than focus on the micro-issue of the effectiveness of export controls, the nation might benefit more from focus on the macro-issue of what technologies are really unknown

477. 15 C.F.R. § 734.8(a)–(b); 22 C.F.R. § 120.11(8). There is a very limited exception providing for a fundamental research exclusion to apply to research satellites and related information exports to certain entities in NATO, major non-NATO ally, European Space Agency, and European Union countries, involving only nationals of such countries. *See* 22 C.F.R. § 121.1(XV)(a), (e), § 123.16(b)(10) (equipment), § 125.4(d) (information). The utility of this narrow exception that extends fundamental research to these friendly locales, however, is extremely limited because the recipients must ensure that the export is only to nationals of the covered countries. *See id*. Our foreign sister universities have as much trouble as we do restricting participation in research, teaching and other activities (e.g., lectures) to nationals of the university's country. American and foreign universities' student bodies, faculties and campus communities are international. Consequently, some colleges and universities have concluded that these exceptions are not at all useful for their researchers in practice.

478. National Defense Authorization Act for Fiscal Year 2000, Pub. L. No. 106-65, 113 Stat. 512 (1999).

479. *See supra* note 54, concerning March 25, 2004, report.

elsewhere, have real likelihood of posing a threat to our national security, and should be classified. The wisdom of this approach was recognized in the mid-1980s with the adoption of National Security Defense Directive 189, which has served our nation and academia well.

The cultures of most academic institutions accommodate openness and publication more naturally than exclusion on the basis of citizenship and secrecy. This principle, which counsels for an approach that fosters exclusion from export controls whenever possible, should guide most college and university export controls compliance programs. Faculty, students, and staff who may be subject to export controls should be well educated on how to ensure that their research and other activities qualify for the public domain/public availability or fundamental research exclusion, and on when to seek expert assessment of whether a license is required before any export or deemed export occurs. The institution's sponsored research office, with support from its counsel's office, can be an effective office for compliance assistance and oversight.

VII. CONCLUSION

Our nation is experiencing an identity crisis of sorts, precipitated by the attacks of September 11, 2001, and pitting the importance of physical security against the foundations of our free society and democracy. The challenges to both are real and cannot be trivialized or ignored. If we are to mature as a nation through these times and still realize the attributes that make us a leader of innovation, prosperity, and justice around the world, we must exhibit wisdom, leadership, and risk-taking of a character that we have not seen in recent history. Academia plays a fundamental role in our democracy and society, as Supreme Court Justice Sandra Day O'Connor recognized in her landmark Equal Protection opinion in the University of Michigan Law School admissions case, *Grutter v. Bollinger*.[480] While Justice O'Connor was referring to only one of the many critical roles the academy fulfills, that of preparing the nation's future citizens, workers, and leaders, she was in some sense reflecting on the importance of academia to our nation's democratic values, economic strength, and national security.

The missions of many of our great academic institutions encompass educating our students to realize their highest intellectual and personal potential and to live a life of value for themselves and others, as well as serving our nation through our education and research programs. In the words of Massachusetts Institute of Technology's mission statement, we are founded to serve the nation by "bring[ing]. . . knowledge to bear on the world's great challenges." More than 150 years of history tell us that American academia has served many of our national

480. 539 U.S. 306, 123 S.Ct. 2325 (2003). In *Grutter*, Justice O'Connor, writing the opinion of the Court, stated that "[w]e have repeatedly acknowledged the overriding importance of preparing students for work and citizenship, describing education as pivotal to 'sustaining our political and cultural heritage,' with a fundamental role in maintaining the fabric of society." (quoting Plyer v. Doe, 457 U.S. 202, 221 (1982)). Justice O'Connor further wrote "[t]his Court has long recognized that 'education . . . is the very foundation of good citizenship.'" *Grutter*, 539 U.S. at ___, 123 S.Ct. at 2340 (quoting Brown v. Bd. of Educ., 347 U.S. 483, 493 (1954)).

interests very well by creating an imperfect, but still great, meritocracy that takes our nation's values of openness, freedom of ideas and expression, hard work, inclusion of people of every color, creed, and nationality, and individual rights to an even higher ideal than is achieved in business or in our society at large. For much of our history, academic institutions have achieved these objectives by creating a rich, varied, and decentralized intellectual environment that benefits from a diverse and international population of students and faculty, and is defined both by individual independence and by openness. Academia has been characterized as an "Ivory Tower,"[481] a place complementary to the rest of American society, but distinct and in many respects insulated from the hierarchy, constraints, and economic profit motive of the world outside our academic fortress. This environment has been a fertile one for creative, fundamental research that is funded by government and industry. Academic fundamental research fuels our government's development of tools for national security and provides fodder for American industry's development of products for the world's markets, as well as for applied medicine, science, and engineering. This environment has depended in part on providing for the needs of our faculties so that they may focus on their teaching and research, unfettered by unnecessary bureaucracy.

The exigencies of the current times have invaded the "Ivory Tower," subjecting academia, on the same terms as the rest of American society, to greater constraints imposed by new and amended federal laws. The USA PATRIOT Act, BPARA, changing policies on the interpretation and enforcement of export controls, changes in laws governing non-immigrants, etc., have created physical security requirements that effectively reduce contact and, consequently, the free exchange of ideas among researchers using certain biological agents and toxins and build barriers between American and foreign students and academics. These legal and policy developments also impose direct prohibitions on the pursuit of, and participation in, certain biological research by some members of our academic communities. Prohibitions on participation are based on immensely broad generalizations about the suitability of individuals of certain nationalities or who may fall within even minor and common categories of mental disorders. In addition, academia is being held to a higher standard of internal controls over compliance with these laws than has been its custom, and is being asked to view the adequacy of its performance from a law enforcement perspective. Our faculties cannot delegate many of these compliance obligations to others and must learn and operate within a new regime of prescriptive rules that divert attention from core research and teaching.

And the trend toward greater security, prescriptive rules (as opposed to general performance standards), exclusion of individuals on bases that have nothing to do with their intellectual capacity, and the like, is increasing. The Inspector General

481. The term "Ivory Tower" comes from the Bible, *Solomon* 7:4, and refers to the beauty of a woman. In 1873, French poet Charles Augustin Saint-Beuve and, in 1916, Henry James used the phrase to describe those who shelter themselves from the real world. The Ivory Tower has come to be known as an "idyllic" place compared with the outside world. *See* Susan A. Holton, *Why an Ivory Tower*, THE NAT'L TEACHING & LEARNING FORUM, *available at* http://ctl.stanford.edu/teach/NTLF/v11n3/view.htm (last visited Apr. 4, 2004).

of the U.S. Department of Agriculture ("USDA") recently found that USDA-funded research involves chemicals and biological agents and toxins that in the IG's view could be used in bioterrorism and are not adequately secured. The implication is that more, or more prescriptive, regulation is needed.[482]

To be fair, not all of the new regulation of academia is precipitated by September 11. After more than a decade of heavy focus on industry, the Environmental Protection Agency ("EPA"), beginning in the mid- to late-1990s, broadened its focus to include the hazardous waste management practices of colleges and universities through the agency's so-called university initiative.[483] For some time, the National Institutes of Health have been focusing on more robust regulation of and training in human subject research and many federal agencies have been focusing on regulation of conflicts of interest in research. And stricter regulation of privacy of student education records and certain health information was initiated some time ago.[484] The objectives of many of the new laws and policies are important ones with which few would argue, but the methods prescribed for accomplishing these objectives do not fit well within our academic culture.

The cost of these federal law and policy changes to our nation must be measured in several ways. Of course there is an economic cost. The Council on Government Relations' ("COGR") May 1, 2003, Report of the Working Group on The Cost of Doing Business, concludes that legal and administrative compliance costs for academic research institutions (including HIPAA, export controls, and compliance office costs) have increased incrementally as a result of greater federal regulation by approximately 23% per year from 2000 through 2005, and related operations and maintenance costs (including utilities, security, renovations, environmental health and safety, hazardous waste, and BPARA costs) have increased incrementally for the same period by approximately 10.6% per year, both without any additional government funding.[485] This increase in costs may cause academic institutions to make choices on what research they will pursue based on whether they can afford the attendant compliance costs, hardly a good

482. *See* John Heilprin, *Bioterror Concerns Raised at Universities*, ASSOCIATED PRESS, Nov. 21, 2003, *available at* http://www.usatoday.com/news/nation/2003-11-21-bioterror-campus_x.htm.

483. *See* Press Release, U.S. EPA, EPA Files Complaint Against Clarkson University for Hazardous Waste Violations (Oct. 30, 2003), *available at* http://www.epa.gov/region02/news/2003/03121.htm (last visited Apr. 4, 2004); Press Release, U.S. EPA, EPA Continues Successful Enforcement Program Nationally and In Region 2 (Dec. 11, 2003), *available at* http://www.epa.gov/Region2/news/2003/03143.htm; Press Release, U.S. EPA, EPA Launches Compliance Initiative Aimed at 258 New England Universities; Fines University of New Hampshire for Hazardous Waste Violations (Mar. 15, 1999), *available at* http://www.epa.gov/region01/pr/1999/031699.html.

484. *See* Bradie Metheny, *Policy in Perspective: Academic Research Crippled by Unfunded Mandates, Administrators Argue*, WASH. FAX, Feb. 2, 2004, *available at* http://www.washingtonfax.com/pl/2004/20040202.html (subscription required). *See also supra* Part IV and note 35 (regarding FERPA and the HIPAA).

485. On file with the Council on Government Relations, *at* http://www.cogr.edu (see "What's New" and "Cost of Doing Business Report").

impetus for making research decisions or one that can be viewed as serving our nation or humanity well.[486]

Academia and government are already opening a dialogue on how to better reflect the cost of compliance in the federal research cost recovery regime; and although the answers are not easy, there is hope that a solution will be found. More difficult to quantify and address are the costs imposed by these new laws and policies on our nation's competitiveness and role in the world as an innovator, economic and education leader, and model of social justice. Many others have cautioned our nation to consider the devastating effects on the Cold War era Soviet Union of that country's isolationist and prescriptive policies when considering the post-September 11 attitude of our own country toward government regulation, international collaboration and individual freedoms.[487]

We cannot fail to appreciate that the very fields that many new regulations constrain, such as biological research, are the fields that offer the greatest promise of new discovery for the betterment of humanity in the coming century. Biological research (including research in biological sciences, medical sciences, other life sciences, and biological and biomedical engineering) has grown at a rate of 97% over the ten years ending in 2001, as compared with all other areas of scientific research and development which grew at a rate of 55%, according to a National Science Foundation survey.[488] And these fields continue to be among the most productive in academic research today.[489] This means institutions that have not yet been heavily affected by the USA PATRIOT Act or BPARA may be more affected in the future.

So, what shall we do as a nation and as an academic community? The federal government, industry, and academia must redouble our efforts to collaborate on ways to achieve important security objectives without undermining the attributes of our democracy and society that make our nation a world leader. Each sector must appreciate the different attributes and roles of the others in perpetuating our nation's economic, education, and social justice leadership, as well as our nation's security. Each sector must appreciate the symbiotic nature of its and the others' roles. It is not easy to achieve the right balance, but it is a worthy and necessary goal. As an academic community, we must exercise leadership to support the long-term good of our entire community and nation rather than attempting to further the immediate goals of a particular institution.

In the meantime, as we face implementation of the many post-September 11

486. *See* Methany, *supra* note 484. ("[I]t is not out of the realm of thinking that many university presidents are going to . . . ask themselves what type of research they can do based on what they can afford.").

487. See Gast, *supra* note 4, and the sources cited in Professor Gast's article. *See also* Daniel J. Kevles, *Biotech's Big Chill*, TECH. REVIEW 7 (July/Aug. 2003) ("Biomedical research in the United States is facing a security clampdown unlike anything seen in science since the dawn of the nuclear age. Physics survived cold-war restrictions, but the effects of current limitations on biotechnology could be far more chilling for U.S. competitiveness.").

488. *See* National Science Foundation, Academic Research and Development Expenditures, 2001, *available at* http://www.nsf.gov/sbe/srs/rdexp/start.htm (last visited Apr. 4, 2004).

489. *Id.*

federal laws and policies on our campuses, we as lawyers and administrators must work in a close partnership with our academic colleagues to design approaches that place as little burden as possible on the academic endeavor and are as sustainable as possible in our academic environment. We exist at our institutions to serve our faculties and student bodies as they realize the core missions of our institutions. Our academic colleagues are inherently creative problem solvers. We must explain what cannot be avoided in the new laws that govern their work, and then enlist their genius to help us devise the best approaches to implementation. Wherever possible, we need to provide several choices in implementation that satisfy legal requirements and will allow sub-cultures within our academies to choose solutions that are as natural as possible for them. This is a time consuming endeavor, requiring great listening skills and a willingness to learn. It is worth the effort because the stakes to our nation and our great academic institutions are so high.

Our challenge is to evolve our institutions to face the new regulatory regimes without changing their most valuable and successful attributes. Our challenge is to use our strengths as educators to better inform the public, the government, and industry about the cost of over-broad and unnecessary constraints on academic freedom and open exchange of ideas and research. Our challenge is to exercise leadership and vision to address the complex and likely long-term risks that threaten our national security as well as our national identity.