Order Code RL31354

Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education

April 8, 2002

Genevieve J. Knezo
Specialist in Science and Technology Policy
Resources, Science, and Industry Division

Possible Impacts of Major Counter Terrorism Security Measures on Research and Development

Summary

The Congress, the executive branch, and scientific and technical communities have adopted and are considering research and development (R&D) and education-related security measures to counteract terrorism. There is widespread agreement on the need for these measures, but some experts say that they could have unintended consequences. Some of these actions are included in the PATRIOT/USA Act, P.L. 107-56; in addition the Office of Homeland Security, federal agencies, and the scientific and technical community have proposed or taken other actions. Activities relating to higher education (in H.R. 3525, S. 1749, and other bills) include controlling the visa entry and educational programs of foreign students and tracking their movement through the higher education system. Activities relating to limiting access to scientific and technical information include controlling access to R&D laboratories, self-policing, classification and reclassification of already released materials, withdrawal of information from federal agency websites, possible additional exemptions to the Freedom of Information Act, (FOIA) and withholding information categorized as "sensitive but unclassified." Legislative proposals dealing with access to biological agents that could be used by terrorists appear in H.R. 3448, S. 1765, H.R. 3160, S. 1635, H.R. 3457, and S. 1764. These include proposals to register users of potentially toxic biological and chemical agents; to inventory laboratories that conduct research using pathogenic biological agents; to limit access to R&D laboratories and biological research agents; and to give tax preferences to firms that develop tools to deal with bioterrorism.

Among the unintended consequences of these actions, as cited by experts, are high financial costs, especially to academic laboratories, of instituting security and tracking measures, the possible deleterious impacts on freedom of scientific information exchange and scientific inquiry, and the possible loss to the United States of foreign technical workers in areas of short supply among U.S. citizens. Policymakers might seek to ensure that those affected by counter terrorism policies that affect R&D – scientists, academics, industrialists, and the public – are involved in security-related decisionmaking and implementation of regulations.

Through "Operation Shield America," the Customs Service has expanded prohibitions on technology exports which terrorists could use. Some say that this might help to prevent terrorism; others say it could possibly reduce the competitiveness of U.S. technology sales in world markets.

The National Academy of Sciences, the American Chemical Society, the American Psychological Association, and other professional groups have offered to assist the government and are monitoring opportunities for their members to compete for federal awards for counter terrorism R&D and related activities. See also *Federal Research and Development for Counter Terrorism: Organization, Funding, and Options*, CRS Report RL31202, which focuses on funding and priority-setting at the interagency level, and on bioterrorism and cybersecurity R&D.)

Contents

Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education

Introduction

Science and technology (S&T) are a double-edged sword in the fight against terrorism – whether at home or abroad. S&T can help prevent and attenuate attacks (communications, surveillance and prevention technologies, public health vaccines, and pharmaceuticals), and defend against enemies (by strengthening the arsenal of weapons). But S&T can benefit the terrorist by providing advanced technologies or weapons – nuclear, chemical, biological, and cyber – and by giving terrorists opportunities to purchase information and products to exploit the vulnerabilities of complex technological systems on which advanced economies depend.[1] "In the next several years," according to John C. Gannon, former chairman of the National Intelligence Council and a former deputy director for intelligence at the Central Intelligence Agency (CIA),

> the continuing revolution in science and technology will accentuate the dual-use problem related to biotech breakthroughs in biomedical engineering, genomic profiling, genetic modification and drug development. Discoveries in nanotechnology and materials science will add to the challenge. Responsible scientists will have an extraordinary opportunity to improve the quality of human life across the planet. At the same time, terrorists and other evildoers may develop a powerful capability to destroy that life. The genetic revolution could transform classic agents, oldie moldies, into custom pathogens resistant to all known treatments.[2]

The fact that science and technology can be used for good and evil poses a dilemma for scientists, government, and industry. Some who seek to deny scientific and technical information to terrorists say this will restrain the free exchange of scientific information, students and researchers, and ultimately inhibit scientific progress. Gerald L. Epstein, with the U.S. Defense Threat Reduction Agency, commented, " 'Our ability to deny access to...weapons, ... is fundamentally limited....'

---

[1]Arnaud de Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, Michèlle M. Ledgerwood, *R&D Needs, Cyber Threats and Information Security Meeting the 21st Century Challenge,* Center for Strategic and International Studies, December 2000, p. 11. See also: Katie Hafner, "In the Next Chapter, Is Technology an Ally?" *New York Times,* Sept. 27, 2001, and "Enemies at the Cutting Edge: Military Policies Are Obsolete. Improved Intelligence Must Become the Mainstay of the West's Future Defence," *Financial Times,* Sept. 26, 2001, p. 17.

[2]John C. Gannon, "Viewing Mass Destruction Through a Microscope," *New York Times*, Oct. 11, 2001.

Much of the relevant equipment is in widespread commercial use and internationally available; the pathogens involved can typically be found in the environment; and the underlying research and technology base is available to a rapidly growing and thoroughly international technical community." He continued, "This means not only that a sophisticated adversary willing to devote sufficient time and resources to developing biological weapons is likely to succeed, but that policy measures to frustrate such developments are likely to affect many legitimate activities outside of the ones they are intended to address."[3]

In a democracy, it is difficult to develop policies that balance security and access to information. Terrorists' actions can not be predicted and need to be thwarted. On the other hand, scientific and technological progress requires information exchange, and economic growth depends, in part, upon commerce in technologically sophisticated goods, which flow from advanced R&D in core fields of science and technology.[4]

Relevant Laws Enacted Before September 11, 2001

Even before the terrorist attacks of September 11, 2001, Congress had enacted laws which sought to enhance the security of some activities relating to science, technology, and higher education. Three salient enactments are described next and will be expanded upon below in this report.

Pursuant to Section 212 of the Immigration and Nationality Act, as amended,[5] State Department consular officials who issue student visas abroad are required to deny visas for U.S. study in sensitive fields and/or areas of illegal export of technology. Under the rules developed by the State Department to implement the law, consular officials may deny visas for study in the United States in 16 categories specified on a *Technology Alert List* to students from countries identified as "state sponsors of terrorism." The seven countries on the State Department's *List of State Sponsors of Terrorism* are Cuba, Libya, Iran, Iraq, North Korea, Sudan, and Syria. In addition, with regard to issuing visas to students who wish to study in these fields, consular officials are to "be alert to cases involving foreign nationals affiliated" with countries subject to the Nonproliferation Export Control regulation, that is China, India, Israel, Pakistan and Russia.[6] The purpose is to avert the spread of weapons of mass destruction and missile delivery systems, maintain U.S. advantage in some militarily critical technologies, and prevent the transfer of arms and dual-use items to terrorist states.

---

[3]Gerald L. Epstein, "Controlling Biological Warfare Threats: Resolving Potential Tensions Among the Research Community, Industry, and the National Security Community," *Critical Reviews in Microbiology*, vol. 27, no. 4, 2001, as described in *Secrecy News*, from the *FAS Project on Government Secrecy*, Vol., No. 6, Jan. 15, 2002.

[4]John Schwartz, "Silver Bullet-ism: Technology Runs to the Rescue," *New York Times*, Dec. 9, 2001.

[5]8 USC 212(a)(3)I)(II).

[6]"Visas Mantis," [http://travel.state.gov/reciprocity/SAO/MANTIS.htm].

Two laws were enacted after the World Trade Center bombing attack in 1993.

One was the "Antiterrorism and Effective Death Penalty Act of 1996," P.L. 104-132, which required the Secretary of the Department of Health and Human Services (DHHS) to identify hazardous biological agents and require registration of laboratories that transported hazardous biological agents. The law did not require registration of laboratories that used any of the "select agents" or reporting of existing inventory in laboratories. Researchers and laboratories that possessed stockpiled strains in freezers but did not plan to transport them did not have to register and report to the government. Biological warfare uses were prohibited.

Second, the "Illegal Immigration Reform and Responsibility Act of 1996," which was part of P.L. 104-208, authorized an electronic foreign student tracking system, called the Cooperative Interagency Program Regulating International Students (CIPRIS) Student Exchange Visa program (SEVIS), was authorized. The electronic monitoring system was intended to make readily accessible to immigration officials the names, residences and educational status of foreign students. The program was not fully implemented before September 11, 2001 largely due to objections from the higher education community about financial costs foreign students would incur as the system was implemented.

Introduction to Current Issues

Since the September 11, 2001 terrorist attacks, Congress, the executive branch, and the scientific and technical communities have adopted additional security measures, or have considered legislative proposals, to counteract terrorism. These include passage of the PATRIOT/USA Act, P.L. 107-56, signed by the President on October 26, 2001, which, among other things, increased foreign student monitoring, restricted access of potential terrorists to hazardous biological agents, and gave the government access to some information about students and their Internet usage. The government has issued regulations and imposed new guidelines about: withdrawing scientific and technical information from federal agency websites and limiting access to "sensitive, but non-classified" information; reclassifying already released materials; limiting access to information accessible via Freedom of Information Act; and expanding the list of technologies subject to export control. Proposals are being considered to limit access to R&D laboratories, expand the list of biological research agents that are controlled, and to register laboratories that conduct research using materials of potential value to terrorists. In addition, some scientists have started to impose self-policing and to develop guidelines relating to release or withholding of certain kinds of scientific and technical information.

While there appears to be widespread agreement on the need for improving security and limiting access, some researchers and academicians assert that certain of these actions could have unintended consequences for the conduct of research and development, training of students, and could impinge upon implementation of existing laws. The efforts to restrict access to scientific and technical information, entry to the United States of students who might be potential terrorists, and use of hazardous biological agents raise several issues. These include the potential to reduce the number of foreign students in science and technology, thereby possibly reducing income to U.S. higher education institutions and, ultimately, the capability of a future

U.S. science and technology workforce. There are issues of constraining scientific information exchange and scientific inquiry; limiting public access to information presented to the Government and sought by the public pursuant to the Freedom of Information Act and the Community Right to Know Act; and determining who bears the cost of increased security for academic laboratories and for screening scientific researchers.

Some in the research community suggest that steps might be taken in implementing these actions to mitigate adverse effects on legitimate researchers and students. This report summarizes the major concerns voiced by professional and technical experts and issues that policymakers and administrators may consider when drafting regulations and implementing policies and programs to ensure security for activities that traditionally have been conducted without major governmental regulation and restraint. (Another CRS report deals with legislation and governmental action to coordinate funding and priority-setting for counter terrorism R&D at the interagency level, and especially for bioterrorism and cybersecurity R&D. See *Federal Research and Development for Counter Terrorism: Organization, Funding, and Options,* CRS Report RL31202.)

This report addresses security actions and issues relating to students in higher education, access to biological agents, access to laboratories, access to scientific and technical information, and new export controls. It also identifies actions of selected professional associations related to counter terrorism R&D.

Impacts of Counter Terrorism Activities on Students at U.S. Universities and Colleges

Definition of the Policy Issue

Accounts of the pilot training received in the United States by the September 11th terrorists underscored the contribution of U.S. training and education to potential terrorists. Concerns were heightened by reports that some terrorists entered the United States on student visas, but never matriculated at the school to which the visa applied. Some fear that foreign students may include terrorists or their sympathizers, who gain entry to the United States for illegal purposes or, who, with the benefit of knowledge and skills gained in the United States, could mount terrorist campaigns. As an example,

> In the 1970s and 80s, [Saddam] Hussein sent scientists to universities in Western Europe and the United States for programs in chemistry, biology and animal and plant pathology. One of them, Rehab Taha, who studied in Britain, became the head of Iraq's biological weapons programs. Many scientists working under Dr. Taha, nicknamed Dr. Death by United Nations weapons inspectors, were also trained overseas. The head of Iraq's nuclear weapons program, Samir al-Araji, earned mechanical engineering degrees at Michigan State University.[7]

---

[7]Diana Jean Schemo, "Access to U.S. Courses Is Under Scrutiny in Aftermath of Attacks," (continued...)

Counter terrorism security actions for U.S. and foreign students at colleges and universities are intended to deny visas to potential terrorists, increase monitoring of students, and prevent potential terrorists from studying "sensitive" subjects and conducting R&D with material that could be used for damaging purposes. These actions are especially pertinent to foreign students who study science and technology, since they now comprise about 30% of graduate students studying science and engineering in the United States and 33% of U.S. science and engineering doctoral recipients. This section begins by describing the presence of foreign students in U.S. science and engineering, addresses actions to control their entry and monitor their access to science and technology courses, and identifies possible unintended consequences of these actions, as suggested by higher education experts and research professionals.

Numbers of Foreign Students Who Study Science, Engineering, and Mathematics

The National Science Foundation (NSF) reported that in 1998, the latest year for which data are available, nonresident aliens, including foreign citizens on temporary visas, comprised almost 4% of students who earned bachelors degrees in science and engineering,[8] about 25% of students who earned master's degrees in science and engineering,[9] and about 30% of the doctoral recipients in major science and engineering fields.[10] Foreign students enrolling in U.S. science and engineering graduate programs under temporary visas in 2000 rose by about 10.9% over 1999 and now comprise about 35% of total graduate enrollment in science and engineering, compared with 24% in 1993.[11] The number of foreign graduate students in core science, mathematics, and engineering fields is about equal to, or exceeds, the number of U.S. students in some subjects, with students on temporary visas constituting well over one-third of all doctoral recipients in major science and engineering fields. **See Table 1**. Some foreign doctoral recipients remain in the United States after receiving their degrees.[12] Increases in the foreign graduate student population may decline,

---

[7](...continued)
New York Times, September 21, 2001.

[8]Table 1, in U.S. National Science Foundation, *Science and Engineering Degrees, by Race/Ethnicity of Recipients: 1990-98,* NSF 01-327 (June 2001).

[9]Table 2 in *Science and Engineering Degrees, by Race/Ethnicity of Recipients: 1990-98.*

[10]Based on data in Table 4, of U.S. National Science Foundation, *Science and Engineering Doctorate Awards: 2000,* 2001.

[11]Joan S. Burrelli, "Growth Continued in 2000 in Graduate Enrollment in Science and Engineering Fields," NSF Data Brief 02-306, December, 21, 2001.

[12]According to NSF's *Science and Engineering Indicators 2000*: "About 53 percent of the foreign students who earned S&E doctorates from U.S. universities in 1992 and 1993 were working in the United States in 1997. The stay rates are higher for scientists and engineers from developing countries such as China (92 percent) and India (83 percent). In contrast, stay rates are lower for those from emerging economies such as Taiwan (36 percent) and Korea (9 percent) that can absorb highly qualified, skilled scientists and engineers." (Source: [http://www.nsf.gov/sbe/srs/seind00/frames.htm], chap. 4.)

according to NSF, as capacity increases in other countries to provide graduate education.[13]

Table 1. Foreign Graduate Students in U.S. Science and Engineering Programs, 2000

	Foreign Students	Foreign Students With Temporary Visas
As a percentage of all U.S. doctoral recipients in U.S. science and engineering programs	35%	30%
As a percentage of all U.S. doctoral recipients in engineering	52%	46%
As a percentage of all doctoral recipients in mathematics and computer sciences	49%	42%
As a percentage of all doctoral recipients in the physical sciences	40%	34%

Introduction to Issues Relating to the Impacts of Counter Terrorism on Foreign Students in Science and Technology

The entry of foreign students to study science and technology is governed by provisions of the Immigration and Nationality Act,[14] which allows consular officials to deny visas to aliens who are viewed as high risks to violate laws relating to the export of sensitive information or technology. In 1996, Congress enacted legislation to restrict visas and eligible fields of study for foreign students and faculty from terrorist countries and to track foreign students. With the passage of the PATRIOT/USA Act after the September 11th attacks, the Congress acted to ensure funding for the tracking system, and to increase federal access to information about students, researchers, and electronic communications. Additional legislation is pending, some of which would tighten security more than existing programs. In addition, pursuant to a Presidential directive, the Office of Science and Technology Policy (OSTP) in the White House, and the Office of Homeland Security have been charged with developing guidelines relating to entry of foreign students. The task force is scheduled to issue draft guidelines in April 2002.

Most educators agree about the need for increased controls on foreign students, and tracking of them and their courses of study in order to help deter terrorism. However, some say it is possible that intensified monitoring of foreign students and

---

[13]Based on data in Appendix table 4-22, in NSF, *Science and Engineering Indicators 2000*, Chap. 4. Some of these data are based on *Science and Engineering Doctorate Awards: 1996, Detailed Statistical Tables,*(NSF 97-329), and NSF, *Statistical Profiles of Foreign Doctoral Recipients in Science and Engineering: Plans to Stay in the United States* (NSF 99-304)

[14]8 U.S.C 212 (a)(3)(i)(II)

their courses of study, as well as the imposition of fees to track students, together with increased controls on sensitive research (which is discussed below in this report), could result in fewer students, especially graduate students, coming to study scientific and technical subjects in U.S. colleges and universities, and ultimately could reduce the supply of scientific and technical personnel available for employment in the United States. This possibility may be considered by policymakers when developing implementing regulations for foreign students. Another CRS report provides a detailed analysis of the issue of foreign students in the United States and issues relating to visas, student monitoring, and related legislative proposals of them.[15]

The *"Technology Alert List"*

Pursuant to Section 212 of the Immigration and Nationality Act as amended,[16] State Department consular officials who issue student visas abroad are supposed to deny visas for U.S. study in sensitive fields and/or areas of illegal export of technology. Under the rules developed by the State Department to implement the law, consular officials may deny visas for study in the United States in 16 categories specified on the *Technology Alert List* to students from countries identified as "state sponsors of terrorism." The 16 categories on the *Technology Alert List (TAL)* are:

1. *Conventional Munitions:* Technologies Associated with Warhead and Large Caliber Projectiles, Fusing and Arming Systems,
2. *Nuclear Technology*: Technologies Associated with the Production and Use of Nuclear Material for Military Applications,
3. *Missile/missile Technology:* Technologies Associated with Air Vehicles And Unmanned Missile Systems.
4. *Aircraft and Missile Propulsion and Vehicular Systems:* Technologies Associated With Liquid and Solid Rocket Propulsion Systems, Missile Propulsion, Rocket Staging/separation Mechanisms, Aerospace Thermal and High-performance Structures
5. *Navigation and Guidance Control:* Technologies Associated with the Delivery and Accuracy of Unguided and Guided Weapons, Such as Tracking and Homing Devices, Internal Navigation Systems, Vehicle and Flight Control Systems,
6. *Chemical and Biotechnology Engineering:* Technologies Associated with The Development or Production of Biological and Toxin Agents, Pathogenics, Biological Weapons Research
7. *Remote Imaging and Reconnaissance:* Technologies Associated with Military Reconnaissance Efforts, Such as Drones, Remotely Piloted or Unmanned Vehicles, Imagery Systems, High Resolution Cameras
8. *Advanced Computer/Microelectronic Technology:* Technologies Associated with Superconductivity Supercomputing, Microcomputer Compensated Crystal Oscillators
9. *Materials Technology:* Technologies Related to the Production of Composite Materials for Structural Functions in Aircraft, Spacecraft, Undersea Vehicles and Missiles,
10. *Information Security:* Technologies Associated with Cryptographic Systems to Ensure Secrecy of Communications

---

[15]Ruth Ellen Wasem, *Foreign Students in the United States: Policies and Legislation*, CRS Report RL31146, Updated Oct. 16, 2001, 12 p.

[16]8 USC 212(a)(3)I)(II).

11. *Lasers and Directed Energy Systems:* Technologies Associated with Laser Guided Bombs, Ranging Devices, Countering Missiles
12. *Sensors:* Technology Associated with Marine Acoustics, Missile Launch Calibration, Night Vision Devices, High Speed Photographic Equipment
13. *Marine Technology:* Technology Associated with Submarines and Deep Submersible Vessels, Marine Propulsion Systems Designed for Undersea Use and Navigation, Radar, Acoustic/non-acoustic Detection,
14. *Robotics:* Technologies Associated with Artificial Intelligence, Computer-controlled Machine Tools,
15. *Advanced Ceramics:* Technologies Related to the Production of Tanks, Military Vehicles and Weapons Systems,
16. *High Performance Metals and Alloys:* Technologies Associated with Military Applications.[17]

As noted above, the seven countries on the State Department's *List of State Sponsors of Terrorism* are Cuba, Libya, Iran, Iraq, North Korea, Sudan, and Syria. In addition, with regard to issuing visas to students who wish to study in the 16 fields, consular officials are to "be alert to cases involving foreign nationals affiliated" with countries subject to the Nonproliferation Export Control regulations. The State Department identifies these countries as China, India, Israel, Pakistan and Russia.[18] The purpose is to avert the spread of weapons of mass destruction and missile delivery systems, maintain U.S. advantage in some militarily critical technologies, and prevent the transfer of arms and dual-use items to terrorist states.

Implications. The White House, reportedly, seeks to enlarge the list of technologies on this list.[19] Principal factors to consider in debating the utility of this list and its possible revision are that: (1) international terrorists could reside in any country, not only those on the list of seven countries; (2) technologies change quickly and the list needs to be monitored and updated to exclude study in newly developed sensitive areas; and (3) the United States needs to assess the balance between rejecting students and allowing entry to them, given that students who do not receive U.S. visas might ultimately choose to study a "sensitive" subject in another country. The Association of International Educators[20] proposed that controls on subjects for study areas need to be "focused and multilateral." This means limiting controls to "narrowly defined sensitive areas with a high danger potential" and negotiating controls "with other countries that are major destinations of foreign students, so we don't end up simply shifting the foreign student business to other countries." It also cautioned that a balance needs to be maintained between openness of the scientific enterprise and undermining of cutting-edge research through excessive control.

---

[17]"Visas Mantis,"[http://travel.state.gov/reciprocity/SAO/MANTIS.htm].

[18]"Visas Mantis," [http://travel.state.gov/reciprocity/SAO/MANTIS.htm].

[19]Chris Adams, "White House Overhaul of Students Visas Is Viewed as Unnecessary by Colleges," *Wall Street Journal,* Nov. 2, 2001.

[20]Concept Paper on "International Student Status," NAFSA, Association of International Educators, Nov. 27, 2001, 4 pp.

(In a related matter, it has been reported that in March 2002, the Defense Department (DOD)[21] proposed a policy – whose text has not been disclosed publicly but which is to be adopted within 90 days – that would restrict foreign nationals from working on sensitive, but unclassified information technology projects. This includes such things as writing software, processing paychecks, tracking supplies and maintaining e-mail systems. The Treasury Department has banned noncitizens from working on communications systems since 1998 and the Justice Department instituted similar restrictions in July 2001. Nevertheless, critics of the DOD policy fault it as xenophobic and short-sighted. Some say that there is a shortage of qualified American citizens to fill many of these jobs (because of the small number of U.S. citizens who study computer sciences), therefore, the jobs will remain unfilled. They also say costs would rise if Americans filled the jobs since they demand higher salaries.[22] The U.S. high-tech industry relies heavily on Indian, Chinese and other Asian workers who enter the United States on special H-1B visas. Many of these visa holders reportedly are employed by the defense sector.[23] Some say that many military computer programs are written by foreign contractors, and that this new policy could jeopardize military capabilities.[24] The Information Technology Association of American (ITAA) argues that such policies "could undermine the nation's long-term security," and "precipitous action here could make it much more difficult and expensive for the military services to acquire the requested TA services." It has urged the DOD to "conduct a full and public assessment of the advantages and risks posed by the current policy and alternative methods to address any concerns."[25])

Foreign Student Visas

After the World Trade Center bombing attack in 1993, Congress authorized creation of an electronic foreign student tracking system, called the Cooperative Interagency Program Regulating International Students (CIPRIS) and later, the Student and Exchange Visitor Information System (SEVIS) (enacted as part of the "Illegal Immigration Reform and Responsibility Act of 1996," which was part of P.L. 104-208). The electronic monitoring system would make readily accessible to immigration officials the names, residences and educational status of foreign students. The higher education community had opposed the system as too costly, intrusive, and burdensome since "...universities [would have] to assume record keeping functions for the [for the Immigration and Naturalization Service (INS) which was to manage

---

[21]Because the policy has not been released, there is uncertainty about its origins. Some news reports say it was developed by the Undersecretary for Acquisition, Technology and Logistics and others say it was developed by the DOD Deputy Director for Personnel Security.

[22]Charles Piller, "U.S. to Curb Computer Access by Foreigners, Government: To Boost Security Some Defense Department Work Will Be Done Only by Citizens," *Los Angeles Times,* Mar. 7, 2002.

[23]Piller, Mar. 7, 2002.

[24]Christopher J. Doobek, "DOD Reviews Systems Access: Draft Policy Could Curb Hires of Foreign IT Workers,"*Federal Computer World, FCW.com,* Mar. 18, 2002.

[25]Letter from Harris N. Miller, President ITAA, to Hon. Edward C. Aldridge, Mar. 18, 2002.

it],"[26] and actions were not initiated to fully implement the system. SEVIS was to be fully operational by 2003.

After the September 11th attacks, Senator Dianne Feinstein stated her intent to introduce legislation to institute a six-month moratorium on the issuance of student visas.[27] She wanted the hiatus to allow time for the INS to implement the electronic foreign student tracking system. The higher education community opposed the proposed visa moratorium,[28] and some professional groups such as the Association of American Universities[29] and the American Council on Education prepared draft opposition letters for college and university presidents[30] expressing the community's concerns to members of the Senate Judiciary Committee. The letter stated that only 1.8% of non-immigrant visas issued in 1999 were educational visas, and that "singling out only student visas for added scrutiny is unlikely to make a significant difference to national security." Instead it recommended

> -more funding to increase significantly the number of State Department consular officials at U.S. embassies to permit more background checks of individuals applying for visas, and
> -more INS funding to permit the prompt implementation of the tracking system.

However, after the September 11th attacks, the Association of International Educators and other groups announced an end to their opposition to the tracking system. Thereafter, academic support increased for monitoring students from the visa application stage through conclusion of their educational program in the United States.[31]

---

[26] Janet Aker, "University Openness Must Not Be Hampered by Visa Crackdown, Says Rep. Boehlert," *Washington Fax*, Oct. 3, 2001.

[27] "Senator Feinstein Urges Major Changes in U.S. Student Visa Program, September 27, 2001," News from Senator Dianne Feinstein, [http://www.senate.gov/~feinstein/releases01/stvisasl.htm].

[28]Dan Curry, "Monitoring of Foreign Students' Status Draws Increasing Attention From Lawmakers and College Groups," *Chronicle of Higher Education*, Oct, 8, 2001.

[29]The National Association of State Universities and Land-grant Colleges (NASULGC) and the Association of American Universities (AAU) created a joint website to document the strategies and policies government and universities have implemented to respond to the September terrorist attacks. In addition, the website includes information on federal legislation and model state legislative proposals, laboratory security, information about federal research opportunities relating to counter terrorism R&D, international students and faculty, campus safety and preparedness, public education activities, electronic surveillance and privacy issues, and statements and op-eds by university presidents and chancellors. The AAU maintains the site [http://www.aau.edu/resources/resources/html].

[30]See: [www.acenet.edu/washington/letters/2001/09september/feinstein.cfm].

[31]Schemo, September 21, 2001; Dan Curry, "Monitoring of Foreign Students' Status Draws Increasing Attention From Lawmakers and College Groups," *Chronicle of Higher Education*, Oct, 8, 2001.

Actions Taken to Increase Student Monitoring

The PATRIOT/USA Act, P.L. 107-56, among other things, extended the student visa monitoring program, which was applicable to U.S. universities and colleges, to include such other educational institutions as "any air flight school, language training school, or vocational school," and authorized appropriations of $36.8 million for implementation of the system to be completed by January 31, 2003. The system will make readily accessible to immigration officials the names, residences and educational status of foreign students. Foreign student fees of $95 will be paid to keep the system operational. Reportedly, while some university administrators still object to the SEVIS monitoring system,[32] many former opponents of the electronic tracking system now endorse it, but object to the fee structure, saying many foreign students will not be able to afford it.[33]

Some academic administrators say it will be difficult to develop an easy-to-operate monitoring system and expand it to include all 74,000 U.S. universities, technical schools and community colleges and have asked the government to provide technical advisory groups, training to implement new requirements, and development of a fee collection system that does not "reduce the number of international students on our campuses because the collection mechanism is unworkable."[34]

The executive branch also took action to increase security surrounding student visas. In October 2001 President Bush issued Homeland Security Directive 2, "Combating Terrorism Through Immigration Policies," a directive ordering Administration officials to conduct a "thorough review" of the nation's student visa system[35] in order to end abuse of student visas. The directive charged the Secretary of State and the Attorney General, together with the Director of the Office of Science and Technology Policy and the Secretaries of Education, Defense, and Energy to develop a program to end abuse of student visas. They are scheduled to issue draft regulations in April 2002. The directive mandated a program to track foreign students who receive a visa, their enrollment status and classes in which they are

---

[32]Abraham McLaughlin, "INS Reaches for High-tech Silver Bullet," *Christian Science Monitor,* March 18, 2002.

[33]"Tracking Foreign Students," AAAS, *Science Technology in Congress*, Nov. 2001. The American Council on Education wrote a letter to the INS Commissioner on February 12, 2002, stating that the $95 fee is too high and should be recalibrated given that Congress provided $36 million to operate SEVIS initially, and that the State Department and the INS should develop a simpler more efficient fee collection mechanism than what is planned in order not to "lengthen the time required for international students to apply, gain admission, and obtain a visa to attend our institutions." Available at [http://www.acenet.edu/washington/letters/2002/02february/ziglar.sevis.cfm].

[34]Kate Zernike and Christopher Drew, "Efforts to Track Foreign Students Are Said to Lag," *New York Times*, Jan. 28, 2002 The details of the academic perspective are in: letter from David Ward, President of the American Council on Education to INS Commissioner James Ziglar Regarding SEVIS, Jan. 24, 2002.

[35]Sara Hebel, "President Bush Orders Cabinet-Level Review of Student-Visa System," *The Chronicle of Higher Education*, Oct. 30, 2001.

enrolled, to identify the source of funds supporting the education, to develop limits on the duration of student visas and "strict criteria" for renewal, to prohibit students from certain countries from studying "sensitive" areas, including those relating to weapons of mass destruction, and to identify "problematic applicants" whose visas should be denied. Shortly thereafter the Justice Department began a program to deport aliens who provide support to certain terrorist groups and to review institutions which might not provide legitimate educational services for foreign students.[36] According to some professional associations, universities and professional societies are not fully involved in these discussions and they fear that they will not be able to participate in decisions made about foreign study entry. Irving Lerch, head of international affairs at the American Physical Society was reported as saying he "fears that the final criteria will curtail recruitment from 'sensitive' countries such as India and China, which supply the United States with large numbers of graduate students."[37]

Pending Legislation: Enhanced Border Security and Visa Entry Reform Act of 2001. Other major legislation regarding student visas and tracking that has received floor action includes the following.

H.R. 3525, similar to the Senate bill, S. 1749, the "Enhanced Border Security and Visa Entry Reform Act of 2001," was introduced by Rep. Sensenbrenner; it passed the House at the end of December 2001 and is pending in the Senate.[38] On March 12, 2002, when passing H.R. 1885,[39] as amended by the Senate, the House amended it by attaching to it H.R. 3525, as previously passed in the House. H.R. 3525 would prevent the government from issuing student visas and other nonimmigrant visas to anyone from one of the seven countries that the State Department considers to be a sponsor of terrorism, unless federal officials first determined that the person does not pose a national security threat. The seven countries on the State Department's *List of State Sponsors of Terrorism* are Cuba, Libya, Iran, Iraq, North Korea, Sudan, and Syria. (Reportedly, "In the 2000-2001 academic year, a total of 3,761 students from those seven countries attended American colleges, according to the Institute of International Education. Of those countries Iran sent the most students, with a total of 1,844.")[40] The bill also requires that students provide information to verify their background, and would require electronic tracking of information about foreign students including visa issuance, date a student enrolls in a college, field of study, and date the student graduated or left the

---

[36]Chris Adams and Jess Bravin, "INS Reviews Student-Visa Policies Amid Tightening of Immigration," *Wall Street Journal*, Nov. 1, 2001.

[37]"Societies Query Student-Visa Review," *Nature*, Mar. 14, 2002, p. 111.

[38]S. 1749, "Enhanced Border Security and Visa Entry Reform Act of 2001, was introduced on Nov. 30, 2001, by Senators Edward Kennedy, Sam Brownback, Dianne Feinstein, and John Kyl. It is a compromise version of S. 1618 introduced by Senators Kennedy and Brownback (House companion is H.R. 3205) and S. 1627, introduced by Senators Dianne Feinstein and Jon Kyl (a similar bill is H.R. 3229).

[39]This bill would extend a program that allows certain illegal aliens and non-citizens who have overstayed their visas to remain in the United States while applying for residency.

[40]Sara Hebel, "House Passes Bill Requiring More Screening and Monitoring of Foreign Students," *Chronicle of Higher Education*, Dec. 21, 2001.

institution. Colleges would have to notify the INS about a student's arrival/enrollment, and the State Department could not issue a visa unless it had evidence that a student had been accepted to an approved academic institution. Until SEVIS is implemented, the bill would set up a transitional student monitoring program. Failure of an institution to comply could result in suspension of the institutions's ability to receive foreign students. The American Council on Education says the initial campus reaction to the compromise legislation is favorable.[41]

There is other related legislation that has not received floor action.[42]

Other Security-related Actions Relating to Students

Three provisions of the PATRIOT/USA Act, P.L. 107-56 have caused concern in the higher education community. These deal with its authorities granting access to student and business records, and the responsibilities it imposes on Internet service providers.[43] Some caution that implementation measures should be developed so as not to remove all privacy protections given to students and researchers in these

---

[41]AAU, *CFR Weekly Roundup*, Nov. 30, 2001.

[42]Other legislation which has not yet received floor action includes:

H.R. 3002 would establish an alien nonimmigrant student tracking system;

H.R. 3004, would establish a student visa tracking system;

H.R. 3033 would authorize appropriations of funds for the foreign student tracking system;

H.R. 3069 would prohibit granting student visas to students from countries on the State Department's list of governments that sponsor terrorism;

H.R. 3077 would expand the current list of approved educational institutions covered in the Immigration Act of 1996 to include flight and language training schools;

H.R. 3181 would institute a nine-month moratorium on the issuance of visas to foreign students;

H.R. 3221 would impose a nine month moratorium on student visas;

H.R. 3222 would limit the number of H1-B nonimmigrant visas issued in any fiscal year;

H.R. 3286 would, among other things, establish a temporary moratorium, with exceptions, on the issuance of visas to aliens from: (1) Afghanistan; (2) Algeria; (3) Egypt; (4) Lebanon; (5) Saudi Arabia; (6) Somalia; (7) United Arab Emirates; (8) Yemen; or (9) any country designated as a state sponsor of terrorism.

S. 1518, would expand the current list of approved educational institutions covered in the Immigration Act of 1996 to include flight and language training institutions, and require university reports on students' failure to begin studies.

[43]AAU, *CFR Weekly Wrapup*, Oct. 12, 2001. For a detailed discussion of the potential impact of the PATRIOT/USA Act on colleges, see: "Colleges Fear Anti-Terrorism Law Could Turn Them Into Big Brother," Transcript of online moderated discussion, CHE colloquy Live, Feb. 27, *Chronicle of Higher Education*, Mar. 1, 2002. For detailed information on the PATRIOT Act and electronic communications, see: *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government*, By Marcia S. Smith, Jeffrey W. Seifert, Glenn J. McLoughlin, and John Dimitri Moteff, CRS Report RL31289, Feb. 12, 2002. 19 p.

areas.[44] These provisions apply to all foreign students, although implementation would focus on students suspected of terrorist activity.[45]

Access to Student Records. Student records, are currently protected by the Family Educational Rights and Privacy Act (FERPA),[46] which prohibited disclosure of student information without consent. According to the Department of Education's Family Policy Compliance Office, institutions may disclose records, without consent, to

- certain government officials in order to carry out lawful functions, individuals who have obtained court orders or subpoenas, and
- persons who need to know in cases of health and safety emergencies.

The PATRIOT/USA Act (Sec. 215), in effect, modified FERPA to expand the ability of schools, without consent of students or parents, to release students' records to appropriate federal officials to aid in the investigation of terrorist activity if approved by a judge. Officials would have to indicate how the information would be used. Liability protection was given to schools that release such records.

Access to Business Records. Section 215 of the law modified the Foreign Intelligence Surveillance Act (FISA) to expand business records that may be accessed by the FBI with judicial approval as part of an investigation to protect against international terrorism or clandestine intelligence activities. Sec. 215 expanded accessible business records to include "... any tangible thing (including books, records, papers, documents, and other items. . .)." Any person who provides such records is indemnified against any liability for doing so. This provision opens business records to greater scrutiny and, according to the Association of American Universities, could provide access to student records, including personal information, such as library use records and medical records.[47]

Internet Service Provider Responsibilities. With respect to online service providers, section 217 of P.L. 107-56 basically expanded the circumstances under which service providers will have to disclose or maintain certain information at the request of government entities. The PATRIOT/USA Act defined new circumstances under which Internet service providers, including universities, may be

---

[44]For a legal analysis of some of these issues, see two documents on the AAU website, "USA Patriot Act: Provisions Governing Electronic Surveillance, Computer Networks, and Privacy Effects of the USA Patriot Act on University Network Service Providers," Mar. 2002 and "The Search & Seizure of Electronic Information: The Law Before and After the USA Patriot Act," Mar. 2002, [http://www.aau.edu/intellect/copyri.html].

[45]Universities are in the process of developing internal regulations to deal with these changes in law. For an analysis of current views and effects on international students, see: Scott Carlson and Andrea L.Foster, "Colleges Fear Anti-Terrorism Law Could Turn Them Into Big Brother," *Chronicle of Higher Education,* Mar. 1, 2002.

[46]20 U.S.C. 1232g, regulations appear at 34 CFR Part 99.

[47]AAU, *CFR Weekly Wrapup*, Oct. 12, 2001.

called upon to permit government agencies without a court order to intercept the wire or electronic communications of persons regarded as computer trespassers. The provisions stipulate that an agent can conduct such interceptions only if the owner or operator of the protected computer authorizes the interceptions, and that the interceptions cannot acquire communications other than those transmitted to or from the computer trespasser. In addition, the term "computer trespasser" cannot include anyone known to have an existing contractual relationship with the computer operators for access to all or part of the protected computer.

Universities were concerned that "... government could pressure service providers (including universities) to ask for assistance as a means for gaining broad authority to intercept an individual's e-mail, websurfing, and other electronic transactions to pursue wider investigations."[48] In addition, some say that the law could penalize legitimate scientific and technical activities. Before enactment of the PATRIOT/USA Act, the U.S. Association for Computing Machinery (USACM) wrote to congressional leaders expressing concern about extending the definition of terrorism to include non-violent computer crimes and "other acts seemingly unrelated to terrorism. USACM also suggested that other broad provisions of the Act could unintentionally include legitimate and ordinary behavior by scientists and technicians." The Association continued by concluding that "Unfortunately, many of USACM's concerns were not addressed as the act become law."[49] Among the other concerns are issues of meeting the costs of expanded information maintenance and assuring that service providers do not have to reconfigure their systems to meet information requests that exceed their current technical capabilities.

Implementation Issues

Many foreign students enroll in U.S. science and technology educational courses and, in some cases, they constitute a major fraction of the graduate student body in core science and technology departments. Some experts contend that counter terrorism actions should be implemented carefully because they might create an atmosphere that is not welcoming to foreign students and researchers, even those from countries not identified as terrorist threats.[50] Citing the potential implications for U.S. academic institutions, the conduct of R&D, and the economy, some argue that caution should be taken in adopting actions which could reduce the numbers or compromise the educational and research activities of foreign students.[51] Many U.S.

---

[48]AAU, *CFR Weekly Wrapup*, Oct. 12, 2001.

[49]*Association for Computing Machinery Washington Update*, Nov. 2001 issue. Letter Oct. 19, 2001 from Co-chairs of U.S. CM Public Policy Committee to Members of Congress.

[50]Reportedly "a sizable number of students from the [Arab] Gulf Region left the United States after the terrorist attacks, and did not return," according to an MIT nuclear engineering professor who was born in Jerusalem (E Masnod, " Blooms in the Desert," *Nature*, March 14, 2002, p. 127.)

[51]Kate Zernike and Christopher Drew, "A Nation Challenged: Student Visas: Efforts to Track Foreign Students Are Said to Lag," *New York Times*, Jan. 28, 2002. See also comments by James W. Ziglar, Commissioner, U.S. Immigration and Naturalization Service, in *National*

(continued...)

institutions encourage foreign student enrollments since foreign students usually pay full tuition and because they keep active some academic departments which might otherwise close for lack of U.S. students. In addition, "an analysis by the National Association of Independent Colleges and Universities shows that although foreign students accounted for 3.4 percent of total enrollment in colleges and universities in 2000, they paid an estimated 7.9 percent of tuition and fees American universities received that year."[52] Some college officials have reportedly argued that if the number of foreign students were reduced, the broader economy could suffer because foreign students and their dependents are estimated to "...pump $11 billion a year into the American economy for tuition and fees, housing, living expenses and consumer goods."[53] In addition, according to one observer, "At many universities, foreign students, particularly from Asia, are a cheap source of high quality research assistance."[54] Some academic critics say that the added cost and new hurdles for foreign study entry presented by counter terrorism security actions could hamper U.S. colleges' ability to compete for top foreign student scholars and researchers, and that the new fee and longer visa-application process could also threaten the existence of some short-term academic programs that cater to international students, such as summer English courses.[55]

There is also the issue of the effects on U.S. science of reductions in the number of foreign students trained here since they make substantial contributions to scientific research.[56] Representative Sherwood Boehlert, chairman of the House Science Committee, cautioned " 'We must not imperil the openness of our universities, which are magnets for students around the world, many of whom choose to settle in the United States.' ...He also pointed out that foreign students are 'absolutely critical elements of our science and technology workforce....' "[57] If the foreign student population in key advanced science, engineering, and mathematics fields in U.S. colleges and universities is reduced, or if many foreign students trained here decide to return to their home country, there is concern that personnel shortages and U.S. capabilities could decline in these areas since U.S. citizens are not attracted to these fields in sufficient numbers to replace foreigners. The argument is also made that training large numbers of foreign students affords many cultural benefits since

---

[51](...continued)
Academies' Report on Post-September 11 Scientific Openness at Universities.

[52]Diana Jean Schemo, "Universities Persuade Senator to Drop Plan to Limit Visas," *New York Times,* Nov. 18, 2001.

[53]Schemo, "Universities Persuade Senator to Drop Plan to Limit Visas," Nov. 18, 2001.

[54]Diana Jean Schemo, "Access to U.S. Courses Is Under Scrutiny in Aftermath of Attacks," *New York Times,* September 21, 2001.

[55]*AAU Public Affairs Report*, December 1, 2001 and Sara Hebel, "Proposed Rules on Foreign Students Leave Many Colleges Worried," *Chronicle of Higher Education,* Oct. 26, 2001.

[56]"Tracking Foreign Students," American Association for the Advancement of Science, *Science Technology in Congress*, Nov. 2001.

[57]"Chairman Boehlert's Speech to SUNY Presidents on the Impact of Terrorism on R&D," Revised, Committee on Science, Press Release, Oct. 1, 2001.

foreigners can learn to understand and appreciate democracy and a capitalist economy.

Other concerns have focused on the costs of implementing monitoring systems, the use and possible expansion of items on the *"Technology Alert List"* to deny student access to "sensitive" subjects for study, and the propriety of increasing access to student records and Internet communications. Implementing regulations may address some of these issues. The National Academies (of Science) held a meeting in December 2001 on the topic of *Balancing National Security and Open Scientific Communications: Implications of September 11th for the Research University*.[58] It focused on three topics: access to scientific information and materials, the flow and tracking of foreign students and scholars; and new fields of study and research needed. The report included recommendations for additional study by the National Academies and other groups.[59]

Security Actions for Biological Agents

Definition of the Policy Issue

The "Antiterrorism and Effective Death Penalty Act of 1996," P.L. 104-132, among other things, required the Secretary of the Department of Health and Human Services (DHHS) to identify hazardous biological agents and require registration of laboratories that transported hazardous biological agents. Specifically, "through

---

[58]Association of American Universities (AAU), "National Academies' Report on Post-September 11 Scientific Openness at Universities," Feb. 6, 2002. Posted at [http://AAU.edu/research/NAReport.html].

[59]The report includes the following recommendations for further study by The National Academies: "In the post...September 11th environment, how can the nation meet its security needs and maintain and develop science and technology for a better, healthy, and efficient society without destroying academic freedom of inquiry and communication? In order to answer this question, we believe there needs to be further study of the following twelve questions .... 1. What information, if any, should be regulated? Which materials, if any, should be regulated? Who should regulate them, and how? ...2. Who should make the decision as to what scientific information and materials are dangerous? ...3. How might it be possible to internationalize norms regarding access to and exchange of scientific materials and information? ...4. To what extent are current non...classified mechanisms used to restrict access to data (e.g., patient confidentiality, proprietary data) useful in the post September 11th context? ...5. Does information regarding chemical or biological agents require special security measures? ...6. Under what circumstances, if any, should publication policies be altered? ...7. If access to knowledge is a right in a democracy, what civic responsibilities come with it? ...8. How can the application of export controls to S&T materials/processes be rationalized? ...9. How can the interested groups-universities, intelligence and security agencies- productively work together on these issues? ...10. How can we strengthen the social/behavioral sciences and the humanities in order to better understand the roots of and responses to terrorism? ...11. How should the scientific community engage the public in these issues? ...12. Are there key areas of scientific research where an infusion of federal funds could make a significant difference in national security?"[http://AAU.edu/research/NAReport.html].

regulations" the Secretary was to "establish and maintain a list of each biological agent that has the potential to pose a severe threat to public safety and health" (Sec. 511 (d)). Section 511(e) required the Secretary to establish "through regulations" safety procedures for transferring listed agents, safeguards to prevent access to such agents by criminals or terrorists, and procedures to protect public safety in the event of a transfer in violation of the safety requirements. The Act also required the DHHS Secretary to "ensure [the] appropriate availability of biological agents for research, education, and other legitimate purposes." The law did not require registration either of laboratories that used any of the "select agents" or reporting of existing inventory in laboratories. Researchers and laboratories that possessed stockpiled strains in freezers but did not plan to transport them did not have to register and report to the government. Biological warfare uses were prohibited. Violators would incur criminal penalties. The law governed the transfer of agents, not the use and possession of them. Many research laboratories that maintain and work with these agents are not registered because they have never shipped them.

Pursuant to P.L. 104-132, the Centers for Disease Control and Prevention (CDC) promulgated a final rule on October 24, 1996[60] that took effect April 15, 1997. Pursuant to sections 511(d) and (e), the regulation included a list of "select" agents (viruses, bacteria, fungi, and toxins, including genetically modified or genetic material from those listed agents),[61] as well as shipping and handling requirements for facilities that transfer or receive select agents. In short, the rule required facilities that ship or receive these potentially harmful agents to register with CDC (and obtain a unique site registration number); disclose the type of agent being transferred, or obtained, and state its intended use; have in place appropriate disposal procedures; and submit to inspections by the agency.[62] The transport of clinical specimens for diagnostic and verification purposes (that is, transport of a patient's blood or tissue

---

[60]*Federal Register* 61: 55189-55200. The rule is codified at 42 C.F.R. 72.

[61]**Viruses:** Crimean-Congo hemorrhagic fever virus, Eastern equine encephalitis virus, Ebola viruses, Equine Morbillivirus, Lassa fever virus, Marburg virus, Rift Valley fever virus, South American hemorrhagic fever viruses (Junin, Machupo, Sabia, Flexal, Guanarito),Tick-borne encephalitis complex viruses, *Variola major* virus (smallpox virus), Venezuelan equine encephalitis virus, Viruses causing hantavirus pulmonary syndrome, Yellow fever virus; **Bacteria:** *Bacillus anthracis, Brucella abortus, Brucella melitensis, Brucella suis, Burkholderia (Pseudomonas) mallei, Burkholderia (Pseudomonas) pseudomallei, Clostridium botulinum, Francisella tularensis, Yersinia pestis;* **Rickettsiae:** *Coxiella burnetii, Rickettsia prowazekii, Rickettsia rickettsii;* **Fungi:** *Coccidioides immitis;* **Toxins:** Albrin, Aflatoxins, Botulinum toxins, *Clostridium perfringens* epsilon toxin,Conotoxins, Diacetoxyscirpenol, Ricin, Saxitoxin, Shigatoxin, *Staphylococcal enterotoxins,* Tetrodotoxin, T-2 toxin. The rule also addresses recombinant organisms/molecule and includes "l. Genetically modified microorganisms or genetic elements from organisms on ...[the list] shown to produce or encode for a factor associated with a disease, 2. Genetically modified microorganisms or genetic elements that contain nucleic acid sequences coding for any of the toxins listed...or their toxic subunits." (Source: 42 CFR 72; see also David Malakoff and Martin Enserink, "Bioterrorism: New Law May Force Labs to Screen Workers," *Science,* Nov. 2, 2001, pp. 971-973.)

[62]The CDC regulations for handling are included in *Biosafety in Microbiological and Biomedical Laboratories*, [www.cdc.gov/od/ohs/biosfty/bmb14/bmbl4toc.htm].

sample from a physician's office to a local laboratory) was exempt from the rule, although isolates of agents from clinical specimens must be destroyed or sent to an approved repository after diagnostic procedures are completed.

The adequacy of these requirements has been an issue.[63] Since the September 11th attacks and their aftermath, legislative attention has focused on expanding the requirements for registration of laboratories beyond transport; identifying and registering laboratories that store and use biological agents that could be used in terrorist attacks; refining lists of toxic biological agents and monitoring their use; and limiting access of unregistered and potentially threatening users to certain biological materials.

Issues relating to implementation of the enacted and proposed legislation focus on: identifying categories of persons who would be allowed or prohibited from working with select agents in U.S. laboratories; identifying and mitigating the financial and "workplace" costs of registering researchers and laboratories; determining whether to expand the list of "select agents;" and determining whether certain categories of clinical laboratories should be exempted from scrutiny.

Provisions of the PATRIOT/USA Act, P.L. 107-56: Registration for Users of "Select Agents"

Section 817 of P.L. 107-56, the PATRIOT/USA antiterrorism act expanded the government's ability to prosecute persons suspected of possessing biological agents to be used for terrorist acts, [64] and addressed some of the limitations perceived in the 1996 law. P.L. 107–56 amended the biological weapons statute[65] to fine or imprison (for up to 10 years) a person who "knowingly possesses 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." In addition, the law criminalized the possession, transport, and receipt of such agents by persons who are under indictment; have been imprisoned for more than one year; are fugitives from justice, unlawful users of a controlled substance, illegal aliens, aliens not admitted for permanent residence from certain terrorist countries where trade is controlled by the Export Administration Act or other related acts, or who have been dishonorably discharged from the Armed Services. Also subject to prosecution for possessing such biological agents under the law, are persons who have been adjudicated as a "mental defective" or who have been committed to a mental institution. No exemptions were specified or permitted; that is, no waiver or appeals process was included.

---

[63]AAU, *CFR Weekly Wrapup,* Nov. 2, 2001.

[64]See also: Scott C. Jenkins, "Antiterrorism Bill May Restrict Bioagency Possession; Research Impact Hazy," *Washington Fax,* Oct. 4, 2001, and William J. Broad, "Experts Call for Better Assessment of Threat," *New York Times,* Oct. 2, 2001.

[65]Chapter 10 of title 18, Sec. 175, United States Code.

Pending Legislation With House or Senate Action: Enhancing Laboratory Security

Whether the PATRIOT/USA Act goes far enough in preventing access to toxic biological materials remains an issue. "Bioterrorism experts have long urged Congress to require researchers who possess deadly materials to register their collections with CDC, and the agency has been embarrassed by its inability to specify how many U.S. labs might have produced the anthrax that has contaminated U.S. mailrooms."[66] The Federation of American Scientists (FAS) took a strong position on biological agents. It described the 1996 regulations "as inadequate because there is no central inventory of dangerous microbes and toxins and because many laboratories that work on anthrax are unregistered."[67] Several bills are pending that would permit enlargement of the list of "select agents," create a national registry to track "select agents," require registration of users, or provide government financial support for registering users and enhancing laboratory security.

Bioterrorism Prevention Act. H.R. 3160, the "Bioterrorism Prevention Act of 2001," introduced by Reps. Tauzin and Dingell, passed in the House on October 23. The bill would extend the regulatory regime established under the 1996 law, P.L. 104-132, by including controls on individuals who knowingly possess listed agents and require them to register with the DHHS. It would make it illegal to possess, use, or exercise control over a biological agent or toxin "in a manner constituting reckless disregard for the public health and safety." Research is not specifically mentioned as an allowable reason for possession, but "prophylactic, protective or other peaceful purposes" are permitted. The bill would allow the Secretary of DHHS to define a broad set of controlled biological agents and toxins, and establish and enforce standards and procedures governing their possession and use. In addition, the bill would prohibit access to biological agents or toxins by any non-U.S. citizen who is not a permanent resident (including individuals in the U.S. on student visas and aliens with non-immigration visas). Illegal possession or transfer of controlled agents would be subject to fines and up to five years in prison. The bill would require any individual who works with select bioagents to obtain a registration from DHHS and would make unregistered possession of these agents a federal felony without requiring proof of intent to use the agent as a weapon. However, the bill would allow the DHHS, in consultation with the Justice Department, to grant waivers for specific classes of visas and specific individuals with "expertise valuable to the United States."[68] Reportedly, this latter clause was added to satisfy those in the pharmaceutical research and academic communities who rely on foreign nationals to conduct research.[69] The bill also would prohibit disclosure under the Freedom of Information Act of information

---

[66]Malakoff and Enserink, Nov. 2, 2001.

[67]Barney Turney, "HHS Evaluating Bioagent Reporting Rules, Which Some Critics Say Contain Loopholes," *Daily Report for Executives,* Nov. 2, 2001, p. A-24. See also: David Malakoff and Martin Enserink, "Bioterrorism: New Law May Force Labs to Screen Workers," *Science,* Nov. 2, 2001, pp. 971-973. This article also identifies the 40 agents subject to control.

[68]Association of American Universities (AAU), *CFR Weekly Wrapup,* Oct. 18, 2001.

[69]Hafner, Oct. 29, 2001, op. cit.

about registered users and laboratories. The bill is now before the Senate Judiciary Committee.

Public Health Security and Bioterrorism Response Act. The "Public Health Security and Bioterrorism Response Act of 2001," H.R. 3448, introduced by Representative Tauzin, deals broadly with public health measures against bioterrorism and also addresses laboratory-security issues. The language is similar to that in S. 1765, introduced by Senator Bill Frist, called the Kennedy-Frist "Bioterrorism Preparedness Act of 2001." (For a detailed comparison of the provisions of these bills by section, see CRS Report RL31263.)[70] Both bills authorize funding to augment specific kinds of anti-bioterrorism and bioterrorism public health activities and, with respect to R&D, would tighten the registration and certification requirements for possessing hazardous pathogens and agents. The bills contain similar provisions giving the DHHS Secretary authority to establish and maintain a list of biological agents and toxins to be listed and regulated, and allow for consultation with professional societies in developing the list. The list is to be reviewed every two years by the Secretary. A database of the location of such agents is to be maintained by the DHHS Secretary under both bills.

Under H.R. 3160 mentioned above, aliens would be excluded as users or registrants or biological agents or toxins that could be used to harm the public health or safety. In contrast, H.R. 3448 and S. 1765 would not exclude aliens as users, but both bills limit access to those "who have a legitimate need for access" in relation to the registration granted. They prohibit use of materials for biological warfare purposes under section 175b of title 18 U.S. Code (for terrorist purposes) and prohibit use by those named in a warrant for domestic or international terrorism. H.R. 3448 also prohibits access to persons under investigation for a terrorist act or suspected of seeking information on biological agents for the intelligence or military operations of a foreign nation. Under H.R. 3448 and S. 1765, the Attorney General is to conduct background screening for registrants. S. 1765 specifies that research-performing organizations, including universities, should be consulted in developing regulations regarding use and transfer of agents. That provision is not in H.R. 3448. Both bills provide criminal and civilian penalties and fines and jail terms for violations. H.R. 3448 gives the DHHS Secretary grant authority to assist public and nonprofit private entities in meeting security requirements for registration. Although there are variations in the language, both bills respond to interests expressed by the professional community to exempt clinical laboratories that use biological agents for diagnosis, verification or testing.[71] Both bills permit DHHS to inspect registered laboratories, and H. R. 3448 makes technical assistance available to laboratories to upgrade

---

[70]C. Stephen Redhead, Donna U. Vogt, and Mary E. Tiemann, *Bioterrorism: Legislation to Improve Public Health Preparedness and Response Capacity*, CRS Report RL31263, Jan. 31, 2002, 34 pp. See especially p. 12 for a detailed comparison of provisions relating to the use and possession of select agents.

[71]Reportedly during a hearing on this proposal, an American Society for Microbiology official recommended that the legislation exempt clinical laboratories "so that facilities engaged in diagnostic work would not have to be specifically registered as long as the samples are destroyed after diagnostic procedures are completed." (Scott C. Jenkins, "Federal Laboratory Bioagent Certification Required Under Planned Legislation," *Washington Fax*, Nov. 8, 2001.)

security. Both bills would also exempt from mandatory disclosure under the Freedom of Information Act, site-specific or identifying information submitted under these regulations concerning registered persons, registered agents and security mechanisms.

H.R. 3448 was passed in the House on December 12, 2001 and referred to the Senate. On December 20, 2001, the provisions of S. 1765 were incorporated into H.R. 3448 (as substitute amendment, S.Amdt. 2692) and adopted. The Speaker appointed conferees from the Committee on the Judiciary for consideration of Title II of the House bill and Secs. 216 and 401 of the Senate amendment, and modifications. It was committed to conference by the House on February 28, 2002. It has been reported that staffers for conferees have been meeting and that the conference to iron out final differences may be held in mid-April 2002.[72]

Related Bills Without Floor Action. Several other related bills have not seen floor action. S. 1706, "Bioweapons Control and Tracking Act of 2001," would require the DHHS Secretary to maintain a list of biological agents or toxins, to review the list periodically, to establish a national data base, and to develop regulations for possession. The bill would impose penalties for violations and would exempt from disclosure under the Freedom of Information Act (FOIA) registration identification information. S. 661 (related bill H.R. 3306), the "Deadly Biological Agent Control Act of 2001," would also prohibit possession and use of listed biological agents and toxins unless for research and requires DHHS certification for users. It would require background checks and allows the Secretary of DHHS to annually assess and review the "select agent" list. Laboratories would be subject to periodic inspection; violators would face penalties.

S. 1635 and the House counterpart, H.R. 3457, "The Pathogen Research, Energy Preparedness and Response Efforts Act of 2001," among other things, would require the Secretary of DHHS to (1) prohibit the unauthorized transportation, by persons who are "nationals of countries which have repeatedly provided support for acts of international terrorism," of chemical agents or biological "select agents;" (2) establish and maintain a list of each biological agent and toxin potentially threatening to public health and another list of those agents and toxins potentially threatening to national security; and (3) establish safety procedures for the transfer of such agents and toxins.

S. 1764, the "Robert Stevens, Thomas Morris Jr., Joseph Cursed, Kathy Nguyen, Ottilie Lungen, and Lisa J. Rains Biological and Chemical Weapons Research Act," introduced by Senator /, would provide incentives to increase research by commercial, for-profit entities to develop vaccines, microbicides, diagnostic technologies, and other drugs to prevent and treat illnesses associated with a biological or chemical weapons attack. It would require the Secretary of Defense, the DHHS Secretary and the Director of the Office of Homeland Security (OHS) to develop and publish a "Biological and Chemical Agent Research Priority List," of agents and toxins that may be used as weapons of mass destruction, and for which tax and patent incentives may be granted for the development of countermeasures for

---

[72]David Glendenning, "Few Hurdles Remain in Merge of Kennedy-Frist, Tauzin-Dingell Bioterrorism Bills, *Washington Fax*, April 8, 2002

approved manufacturers. It included an initial list of 43 biological agents (including many of those on the CDC "select agent" list) and chemicals to be considered.[73] Private organizations that sought to conduct R&D to develop countermeasures for these agents would register with the Food and Drug Administration (FDA) and be subject to inspection. The bill would extend patent term protection to include the full time a product spends in the investigational new drug and new drug application review stages and the bill would provide certain liability and indemnification protection to private research companies. The NIH director would be authorized to support upgrades of certain biological research facilities; NIH would be authorized $200 million to award partnership challenge grants to promote joint ventures between NIH, grantees, and for profit firms to develop biological counter measures.[74]

Implementation Issues

Implementation issues for actions and proposals addressing security for bioterrorism focus on the PATRIOT/USA Act; implications for possibly impeding legitimate research; financial and "workplace"costs of screening and registering researchers; possession of "biological agents" for non-research purposes; questions about exempting some laboratories from security rules; disagreement about items on the "select agent" list; and questions about whether CDC should be given an inspection role.

Possible Constraints on Legitimate Scientific Inquiry, and Financial and "Workplace" Costs. The research community, especially the American Association of Universities (AAU) and the American Society for Microbiology, have sought to mitigate some of the restrictions placed on researchers in some of the pending legislation.[75] The AAU and the FAS sought the exclusion adopted in Section

---

[73]Including agents which are chemicals, that is "Nerve agents (including tabun, sarin, soman, GF, and VX); Blood agents (including hydrogen cyanide and cyanogen chloride); Blister agents (including lewisite, nitrogen, and sulfur mustards); Heavy metals (including arsenic, lead, and mercury); Colatile toxins (including benzene, chloroform, and trihalomethanes); Pulmonary agents (including phosgene and chlorine vinyl chloride); and Incapacitating agents (BZ)."

[74]See also: Lauren Hafner, "Incentives to Lure Private R&D on Countermeasures for Bioagents and Toxins Part of Lieberman Bill," *Washington Fax,* Dec. 14, 2001.

[75]The AAU expressed support for S. 1765, the Kennedy-Frist bill, but raised questions about it, including the following:

> The broad anti-terrorism bill that has already been enacted prevents certain "restricted individuals" (such as felons, fugitives from justice, and others) from handling or using specified hazardous agents. Additional legislation is necessary to clarify how these restricted individuals are to be identified, e.g. background checks. S. 1715 [supplanted by S. 1765 and passed in the Senate] provides that the Justice Department will perform background checks. Can the legislation provide flexibility so that a university may elect to perform background checks itself on individuals who handle or use biological agents or toxins, rather than having the Justice Department perform the background check?

(continued...)

817 of P.L. 107-56 that permitted possession of biological agents for "bona fide research" purposes.[76] Nevertheless, some believe that the PATRIOT/USA Act contains insufficient protections for researchers and imprecision about the definition of research, which federal agencies will have to confront when implementing the law and issuing regulations to administer it. For instance, concerns have been raised about whether subjectivity that could be used in interpreting "bona fide research" as a legitimate exclusion could constrain some scientific inquiry.[77]

Because the new law prohibits certain categories of persons from possessing biological agents that could be used as weapons, including drug abusers, persons who have been committed to a mental institution, and so forth, universities and private laboratories whose researchers would need to meet the qualifications for possession, may need to conduct background eligibility checks and perform drug screening tests on thousands of scientists and students who conduct research on the select agents on the CDC's government's watch list.[78] Academic institutions probably will need guidance on which information to gather from researchers to satisfy the law's user registration requirements.

---

[75](...continued)

> Is there any way to establish a mechanism to grant waivers for individuals who may fall under the "restricted persons" provisions of the broad anti-terrorism bill, but who may nevertheless have valid reasons to use these agents for research purposes? Also, is there any appeal mechanism for individuals whom the Justice Department may find ineligible to carry out such research?
>
> What are universities' obligations to ensure that researchers do not fall under one of the categories of "restricted persons" (such as drug use) that may not be ascertainable through existing federal databases?
>
> Will adequate funding be provided to the Justice Department to perform the background checks? Also, can assurance be provided that the background checks will indeed be performed promptly and will not impede ongoing research?....

(Source: Nails Hasselmo, President AAU to Honorable Bill Frist, Nov. 28, 2001. The text of the AAU letter to Senator Frist was posted on the AAU website under "Research Issues--Campus Lab Security." Source: AAU, *CFR Weekly Roundup,* Nov. 30, 2001.)

[76]AAU, *CFR Weekly Report,* Oct. 16, 2001.

[77]Lauren Hafner, "Bioagent Research, Including Foreign Nationals' Access, Appears Secure for Now Under Patriot Act," *Washington Fax,* Oct. 29, 2001. She reported: "Following the Senate vote on the bill, Sen. Patrick Leahy, D-VT, the sponsor of the first Senate bill, [S. 1510] hinted additional work may be required to ensure the protections for research laid out in the bill are properly codified. The 'bona fide research' exclusion 'may yet prove unworkable, unconstitutional, or both,' he remarked in an Oct. 25 floor statement. Because of his concern that the 'subjectivity' of the standard for violation of the new prohibitions on possession could 'have a chilling effect upon legitimate scientific inquiry,' Leahy called upon the research community and the Justice Department to collaborate on alternative language to 'provide prosecutors with a more workable tool.' " See PATRIOT/USA Act of 2001, Remarks on the Senate Floor by Senator Patrick Leahy, *Congressional Record,* Oct. 25, 2001, pp. S10997-S10998.

[78]Malakoff and Enserink, Nov. 2, 2001.

The Association of American Universities (AAU) objected to both H.R. 3448 and S. 1765. Both, it said, refer to Sec. 817 of the PATRIOT/USA Act, which restricts certain categories of individuals from having access to, or conducting, research on certain biological agents and toxins. But "...neither...includes waiver or appeal processes for these restricted persons, though the research community had sought both. With a waiver process in place, restricted persons who pose no security threats but are key to making research advances might still be able to contribute to searches for vaccines and cures. An appeal process would allow for correction of mistakes. The university research community is working to have language incorporating the desired waiver and appeal processes include in the final conference report."[79]

It has been estimated that up to 250 to 300 universities and additional state and federal laboratories[80] transport "select agents," and have been required to comply with the P.L. 104-132, the 1996 law. Many of these laboratories already screen workers who do classified work for the military or for federal drug studies. But many laboratories do not.[81] According to the Congressional Budget Office (CBO) in its cost analysis of H.R. 3160, it is likely that "tens of thousands" of additional laboratories would be required to screen users under the broader requirements that cover possession.[82] Some fear the security provisions may go too far and claim that background checks might be considered intrusive and affect "workplace morale," since they require information about personal history and behavior. Others believe the research establishment will have to accommodate these upgraded security requirements if the country is to minimize risks of chemical or biological attack. There is also concern that the costs of background checks could become burdensome, especially for academic laboratories. In addition some fear the costs of security and inspection requirements could displace funds that would go to support R&D to combat terrorism.[83]

Difficulty of Restricting Access Without Impeding Research to Combat Terrorism. Some have argued that it is difficult to restrict access to potential bioterrorists as is implied in the legislative proposals as discussed above and that to do so could compromise legitimate counter terrorism R&D. According to Ronald M. Atlas, an official of the American Society for Microbiology in testimony before the Senate Judiciary Committee:

> Implementation of restrictive controls to impede access to biological agents is inherently difficult and potentially could also deter the critical research and

---

[79]"Waiver and Appeals Urged for Bioterrorism Bills," *AAU Washington Report,* Mar. 13, 2002.

[80]Malakoff and Enserink, Nov. 2, 2001.

[81]Malakoff and Enserink, Nov. 2, 2001.

[82]U.S. Congress, House, Committee on Energy and Commerce, *Amending the Antiterrorism and Effective Death Penalty Act of 1996...., Supplemental Report [to accompany H.R. 3016],* House Report 107-231, pt. 2, Nov. 6, 2001, p. 4.

[83]John Fialka, "U.S. Begins Testing Security Systems of University Labs That Use Anthrax," *Wall Street Journal,* Dec. 24, 2001.

> diagnostic activities to combat terrorism. Much of the material and equipment is in widespread use and commercially and internationally available; dangerous pathogens are naturally occurring; and, the research and technology knowledge base relevant to biological weapons is publicly available.[84]

Questions About Legitimacy of Possession by Foreigners of Substances Approved b FDA, but on the CDC's Select Agent" List. Concern has been voiced that more restrictive language relating to registration of users could criminalize possession of some substances for innocent uses not identified in the law or subject to interpretation. For instance, some biological agents, like the botulinum toxin, have medical and cosmetic uses, but can also be used as weapons. In some proposals discussed above, persons visiting the United States on business, tourist and student visas could not use such agents and the government would not have to prove that the person intended to use the toxin as a weapon.

The Food and Drug Administration (FDA) approved for cosmetic purposes products containing "Botox,' which contains the botulinum toxin. The deadly toxin is on the CDC "select agent" list of regulated organisms, and the military is attempting to develop a vaccine to protect troops against it and its paralyzing effects (which for cosmetic uses may eliminate frown lines by immobilizing muscles in the face and other areas of the body). The Commerce Department has imposed civil penalties on U.S. companies that have exported it after finding they did not obtain the requisite export licenses.[85] Some experts question the FDA's approval of botulinum toxin for legitimate uses because of its potential misuse. Dr. Donald Kennedy, a leading biological researcher and editor-in-chief of *Science* magazine, argued that the manufacturer of Botox may be "exploring the development of recombinant strains that might, for example, produce longer-lasting paralysis." As the number of Americans getting Botox treatment increases from the current 1 million to 10 or 20 million, he asked "will we be happy to have that many of these hot bugs around?" He argued that the FDA "should do a comprehensive and careful review of the risks and benefits from extending its approval of botulinum toxin to cosmetic use. "Who would have imagined a world in which terror weapons are employed as beauty aids?"[86]

Questions About Need for Foreigners to Do Research With "Select Agents" to Develop Weapons Against Bioterrorism. The argument has been made that some proposals to restrict access to biological "select agents"could limit the ability of noncitizens to gain access to legitimate biological research in U.S. universities or laboratories. "Dr. Robert Rich, president of the American Society for Microbiology" has been described as being "concerned about possible restrictions on foreign-born graduate students and scientists with keys to university labs. 'They are essential to American science,' he argued."[87] Others say foreigners should not be

---

[84]Atlas' s testimony appears at: [http://www.senate.gov/~judiciary/te110601f-atlas.htm]. Cited in *Secrecy News*, the FAS Project on Government Secrecy, Dec. 12, 2001.

[85]Robert Pear, "Congress Acts to Tighten Toxin Laws," *New York Times*, Oct. 12, 2001.

[86]Donald Kennedy, "Beauty and the Beast," *Science*, Mar. 1, 2002., p. 1601.

[87]Fialka, Dec. 24, 2001.

restricted from using some "select agents" since they are the scientists with the most knowledge of exotic diseases pathogens that are prevalent in foreign countries.[88]

Reportedly, the Administration seeks to have scientists in other countries become subject to analogous registration procedures to handle toxic biological agents as those imposed on scientists in the United States. This is offered as an alternative to the proposed Biological and Toxin Weapons protocol, which the United States has not signed[89] because the U.S. Government objects to opening up laboratories to international inspection, reportedly to protect the proprietary interests of private pharmaceutical firms.[90]

Exempting Some Laboratories From Registration Requirements. There is also disagreement about exempting some researchers and uses from registration requirements. Under the 1996 law, almost all the laboratories in the nation, except those that transport "select agents," are exempt. The exemptions also include clinical diagnostic laboratories. Under P.L. 107-56, certain classes of researchers are prevented from possessing harmful substances that could be used for purposes of terrorism. Pending legislation, such as H.R. 3448, H.R. 3160, and S. 1765, would expand prohibitions on researchers and present additional requirements for laboratory registration, implying that additional laboratories would be monitored. However, certain clinical uses would continue to be exempt. An official of the Federation of American Scientists questioned exemptions for clinical laboratories and asserted that " 'hundreds' of labs around the nation – hospitals, government contractors, and universities – are working on anthrax. There is also considerable informal trading of biological specimens among researchers around the country."[91] According to one report, the FBI says there are about 22,000 such sites, including

---

[88]Andrew Pollack, "Scientists Ponder Limits on Access to Germ Research," *New York Times,* Nov. 27, 2001. See also Jonathan Knight, "Crackdown on Hazardous Agents Raises Concern for Bona Fide Labs," *Nature,* Nov. 1, 2001.

[89]Martin Enserink and David Malakoff, "Bioterrorism: Congress Weighs Select Agent Update," *Science,* Nov. 16, 2001, p. 1438.

[90]

The 1972 Biological and Toxin Weapons Convention (BWC), that 143 nations have ratified, prohibits the development, production and possession of biological weapons. International discussions about compliance measures for the treaty "stalled during the summer of 2001 when the U.S. delegation withdrew because of concerns that enforcement measures – such as lab inspections by an international team "– might compromise national security and threaten biotech companies." (Eliot Marshall, "Counterterrorism: U.S. Enlists Researchers as Fight Widens Against Bioterrorism," *Science*, Nov. 9, 2001, pp. 1254-1255.) At a November 19 review conference in Geneva, the U.S. was to present several alternative proposals, including one proposing criminalization for such possession, one to allow nations to extradite for prosecution those who mishandle biotoxins and cross national borders, and another to devise a "code of ethical conduct" for bioscientists. The U.S. still rejects inspection of laboratories as favored by other countries. (Patrick E. Tyler, "Bush, In Reversal, Seeks Rules for Enforcing Biological Treaty," *New York Times,* Nov. 2, 2001). This has been attributed to the United States government responding to the pharmaceutical industry that opposes inspections of its factories saying secrets can be stolen (Andrew Pollack, "Scientists Ponder Limits on Access to Germ Research," *New York Times,* Nov. 27, 2001).

[91]Turney, Nov. 2, 2001.

small veterinary operations.[92] An issue to be considered in implementation is to ensure that agencies prohibit potential terrorists from benefitting from uses and users exempted from regulation.

Items on the "Select Agent" List and CDC's Inspection Role. There is disagreement about language in some pending legislation mandating the DHHS to revise its select agent list every two years. Experts say that developing the list was not easy in the first place and there are likely to be technical disagreements among bioweapons experts about adding or deleting items. For instance, some U.S. scientists had objected to including Western equine encephalitis on the U.S. list and it was excluded. But other groups include it.[93] Objections have been raised to including *Coccidioides immitis*, on the grounds that laboratories that use it are not required to screen anyone having access to the labs, it is easily grown from desert soil, it is an unlikely choice as a biological weapons since allegedly the illness it causes is mild, and its infection rate is low.[94] Different lists of "select agents" are maintained by "a loose consortium of 34 countries that works to limit the export of biothreats, called the Australian group." It includes as "agents" food-and waterborne diseases such as salmonella and cholera, that are absent from the CDC list. The North Atlantic Treaty Organization (NATO) meanwhile, "has its own lists that include dengue and influenza....."[95]which are not on the CDC list. Some suggest splitting the U.S. list into two classes, with the riskier agents subject to more stringent regulation. There are also questions about whether the select agent list would have to be continuously updated to allow for genetic alterations, such that modified organisms might be considered new agents and thus exempt from the regulations.[96]

It was suggested at the National Academies December 2001 meeting on scientific openness at universities that "A review of the CDC list of select agents should be conducted with an eye to differentiation between the actual risk (that some agents might become weapons and also importantly, that some areas of critical research will become too difficult to pursue as a result of restrictions) versus the benefits (preventing weaponization and facilitating research on pathogenic organisms and emerging infections). A similar review of chemical agents...may be needed as well."[97]

---

[92]Fialka, Dec. 24, 2001.

[93]Enserink and Malakoff, Nov. 16, 2001, p. 1438.

[94]Joshua Fierer and Tho Kirkland, "Questioning CDC's 'Select Agent' Criteria," *Science,* Jan 4, 2002, p. 43.

[95]Enserink and Malakoff, Nov. 16, 2001, p. 1438.

[96]Eugene Russo, "Governing the Dark Side of Science," *The Scientist*, Jan.21, 2002.

[97]*National Academies' Report on Post-September 11 Scientific Openness at Universities,* op. cit. Dr. Charles Vest of MIT proposed to categorize chemical agents along with biological agents. As noted above, S. 1764 would provide preferential tax incentives for development of counter-terrorism technologies, including those relating to the chemicals listed in the bill. For a discussion of the need to develop controls against the use of chemical agents as terrorist weapons, see: James M. Tour, "Do It Yourself Chemical Weapons," *Chemical and* (continued...)

In addition, "Administration officials have also floated the ideas of setting up a new enforcement office within HHS to police microbe research, because CDC, a public health agency, has traditionally resisted that role," because it says it is not a regulatory agency.[98] Questions could be raised about whether CDC's culture and resources are adequate to take on an inspection role.

Restrictions on Laboratories

Definition of the Policy Issue

The fight against terrorism also involves actions to increase federal surveillance of, and to limit access to, some non-biological and biological laboratories, including academic laboratories, both to ensure security of science and technology information that should be withheld from potential terrorists and to investigate the source of anthrax used in terrorist attacks. Issues that could be considered in administering the measures adopted focus on costs to laboratories to prepare for security investigations and enhance physical security, and on access for legitimate researchers so as not to impede scientific research.

Heightened Security and Limitations on Access

Some federal laboratories have limited public and visitor access to their campuses. For instance, on September 20, 2001, Fermi National Accelerator Laboratory announced that, in response to heightened security concerns, it would institute security measures, severely restricting public access to the laboratory. Cultural activities, all non-school related tours, and other access to the site would be prohibited except to employees, visiting scientists and those with official business.[99] The DOE national security programs now fall within the purview of the National Nuclear Security Administration (NNSA), which began operation on March 1, 2000. Some NNSA programs are conducted at DOE civilian R&D laboratories. Because of heightened security, some have suggested that procedures could be developed to ensure that the defense and civilian aspects of R&D are kept strictly separated and that foreign nationals do not get inappropriate access to defense work.

The National Institutes of Health (NIH), which had an open campus before September 11, closed seven of its entrances and now allows visitors to use only one entrance. The agency was advised by the Advisory Committee to the Director of NIH to establish a perimeter defense around the campus and to close other NIH sites

---

[97](...continued)
Engineering News Online, July 10, 2000, pp,. 42-45.

[98]Enserink and Malakoff, Nov. 16, 2001.

[99]"Fermilab Closed to Public Over Security Concerns," *Daily Herald,* Arlington Heights, Il, September 21, 2001, and Fermi National Accelerator Laboratory Press Release 01-27, September 20, 2001.

located outside of Bethesda.[100] NIH is planning to allocate substantial resources to improve its security, according to NIH Associate Director for Research Services, Stephen Ficca. No precise estimates of costs of NIH security upgrades have been made public.

Many academic laboratories have also been required to upgrade security or to adopt measures which they believe reduce potential threats or public fears. Reportedly, after the Iowa Governor called out the National Guard to monitor facilities where anthrax cultures were stored at the Iowa State University in Ames, the school's "microbiologists decided that keeping anthrax spores as part of their general bacteriological collection was more trouble than it was worth. So on 12 October they autoclaved the entire anthrax collection." [101] Improving security does not come without fiscal implications. For instance, it was reported that Northern Arizona University in Flagstaff spent about $50,000 on security upgrades for facilities where live anthrax cultures were used – for new door locks, a wall, and security guards.[102] Glen N. Gaulton, vice dean for research and research training at the University of Pennsylvania Medical School, is reported to have estimated that "the University of Pennsylvania may have to spend $5 million for security features like special filters and pressurized air for handling the 40 agents that can be used to make biological weapons — particularly if Congress rules that researchers working on any genetic or molecular pieces of a lethal organism must take the same precautions as scientists working with the organism in its entirety."[103]

Laboratory Surveillance

In an effort to track down the source of the fall 2001 anthrax attacks, the FBI started to probe many of the over 250 research laboratories across the country that are registered to transport dangerous organisms.[104] The FBI reportedly requested lists of employees, a description of the strains of anthrax used at each facility, and other details. Laboratories under surveillance included federal and academic laboratories, such as Brookhaven National Laboratory in New York and Louisiana State University in Baton Rogue. In November 2001, the FBI issued a subpoena, asking all laboratories in the nation to provide the names of all staff who had been vaccinated against anthrax.[105] The media have reported that the Department of Health and Human Services' inspector general's office instituted new security reviews at

---

[100]Nura Shehzad,"Solid Perimeter Defense Will Transform College Feel of NIH Campus, Kirschstein Laments," *WashingtonFax,* December 10, 2001.

[101]Joshua Gewolb, "Bioterrorism: Labs Tighten Security, Regardless of Need," *Science,* Nov. 16, 2001, p. 1437.

[102]Gewolb, op. cit.

[103]Diana Jean Schemo, "A Nation Challenged: Laboratory Security: Bill Would Require Laboratories to Adopt Strict Security," *New York Times,* Jan. 25, 2002.

[104]Eliot Marshall, "Counterterrorism: U.S. Enlists Researchers as Fight Widens Against Bioterrorism," *Science,* Nov. 9, 2001, pp. 1254-1255.

[105]William J. Broad, David Johnston, Judith Miller and Paul Zielbauer, "Experts See F.B.I. Missteps Hampering Anthrax Inquiry," *New York Times,* Nov. 9, 2001.

academic laboratories and investigators "have begun testing the security systems that are supposed to protect university laboratories from thefts of anthrax, and some 30 other biological agents that terrorists could use. ...[I]n a sign of the times, President Bush gave the HHS power to invoke military secrecy about its university probes."[106] Teams of inspectors from the DHHS's Office of the Inspector General started inspections at universities, including the University of Texas Medical Branch at Galveston. A spokesman for Representative Billy Tauzin reportedly said that Congress has held many security briefings with DHHS on the security of laboratories and that DHHS inspectors are investigating the security of biological samples and of computer data. He noted that DHHS was not releasing a list of laboratories which are being inspected.[107]

Implementation Issues

Details about federal government surveillance of research laboratories are still being developed.[108] While most observers agree there needs to be increased vigilance, improved security measures, and restriction of access to eliminate entry of potential terrorists to research laboratories, some say that science is being over-regulated and that increased controls could ultimately inhibit researchers and compromise the

---

[106]John Fialka, "U.S. Begins Testing Security Systems of University Labs That Use Anthrax," *Wall Street Journal,* Dec. 24, 2001. See also: Kris Axtman, "Campus Labs Eyed After Anthrax Scare," *Christian Science Monitor,* Dec. 10, 2001. According to the Council on Governmental Relations (COGR), an academic and research university professional group, the DHHS review of academic laboratories will examine the following:

> 1. Compliance with 1996 Anti-Terrorism Act provisions. Specific issues include registration of facilities with the CDC, procedures for tracking and reporting of transfers of select agents, and the question of whether the labs are properly equipped to handle and safeguard the materials.
> 2. Compliance with the USA PATRIOT Act. The main focus here will be on the restriction on access to select agents by individuals from the seven countries listed in the Act. If directed, the IG could also review other aspects of the Act, such as mechanisms in place to deny access to select agents to individuals that are convicted felons, illegal drug users, those dishonorably discharged from the military and others designated in the Act.
> 3. The physical security of labs that house select agents and the buildings the labs are in.
> 4. Information technology security for research data related to select agents.

(Source: AAU, C*FR Weekly Roundup*, Nov. 30, 2001)

[107]University Labs Inspected for Bioterror Risks," *CNN.Com*, December 12, 2001.

[108]It was reported in the news that in February 2002, the Justice Dept. started "...sending subpoenas to microbiology laboratories across the country for samples of the Ames strain of Bacillus anthracis, the kind used in the letter attacks in the fall. Scientists working for the ..government said they hoped that studying the samples' genetic fingerprints would help determine which of 12 or more laboratories is the likely source of the bacteria in the attacks." (William J. Broad, "A Nation Challenged: The Anthrax Trail; Labs Are Sent Subpoenas for Samples of Anthrax," *New York Times*, Feb. 27, 2002.

conduct of research.[109] Some college and university officials say that laboratory reviews are being conducted unevenly. In an effort to guide its member institutions, the American Council on Education sent all college and university presidents a letter that discusses the issue of secure handling of biohazardous materials, together with information about federal requirements, and urged that schools take "extra care" in handling these materials.[110] Other college administrators have raised the issue of the costs, in time and personnel of providing information about researchers and laboratory security measures to investigators. Reportedly, some critics seemed assuaged about the potential for more coherent reviews after the selection of a noted bioterrorism expert, Donald A. Henderson, as head of DHHS's new Office of Public Health 'Preparedness.[111]

Some U.S. bioweapons scientists have expressed the view that recent increases in funding for bioterrorism R&D at NIH (about a sevenfold increase in the National Institutes of Allergy and Infectious Diseases which conducts most bioterrorism R&D) "will stimulate the proliferation of labs that handle dangerous pathogens, and raise the risk of an accidental or deliberate release."[112] Some say the money cannot be absorbed effectively and will lead to the support of "bad science." Others argue that security controls are adequate and that "most biological agents pose only a limited threat without the technology to turn them into weapons...."[113]

Restrictions on Access to Scientific Information

Definition of the Policy Issue

Traditional attitudes about open access to scientific and technical information have begun to be challenged since the terrorist attacks, and actions have been taken to keep potential terrorists from gaining knowledge that could be used to attack the United States. Debates about how security can be accomplished without compromising scientific inquiry, the pubic right to information, and public participation in governmental, especially regulatory, processes[114] raise fundamental questions about how much the nation should limit the freedom of scientific information exchange, scientific research (especially basic research), and publication, which traditionally has occurred without governmental control. Proposals have been

---

[109]Willie Schatz, "When the FBI Asks, Should Scientists Tell?'" *The Scientist*, Jan. 21, 2002and Willie Schatz, "Security Fears Put Scientists Under Scrutiny," *The Scientist*, Jan. 21, 2002.

[110]AAU, *CFR Weekly Wrapup*, Nov. 2, 2001.

[111]Marshall, op. cit., and Jim Yardley, "At an Anthrax Lab, the World Changed Quickly," *New York Times*, Nov. 21, 2001.

[112]Jonathan Knight, "Biodefence Boost Leaves Experts Worried Over Laboratory Safety," *Nature*, Feb. 14, 2002.

[113]Knight, Feb. 14, 2002.

[114]Diana Jean Schemo, "Access to U.S. Courses Is Under Scrutiny in Aftermath of Attacks," *New York Times*, September 21, 2001.

made for scientists to self-police themselves to or establish disciplinary groups to develop policies to restrict release of scientific findings. The government seeks to withhold information categorized as "sensitive, but unclassified"; some civilian agencies have been given classification authority that they did not previously have; agencies have been told to reclassify certain declassified materials, and many agencies have removed from their websites information which could be potentially useful to terrorists. Several legislative proposals would extend exemptions under the Freedom of Information Act to restrict disclosure of some R&D-related information. These issues are discussed next.

Self-Policing and Censorship

Self-policing by scientists and professional groups and proposals to withhold or classify scientific information have developed as an salient option since the September 11, 2001 attacks. There are several examples of possible inappropriate use of scientific information by potential terrorists. For instance, some say that conceivably the September 11, 2001 terrorists could have perfected their aeronautical and targeting skills on a computer game called *Microsoft Flight Simulator*, which provided a means for target practice against a virtual Twin Towers.[115] Others claim that the terrorists could have predicted damage patterns in the World Trade towers by using "software marketed [by a U.S. company] under the trade name LSDYNa – an unclassified outgrowth of research on blast effects at Lawrence Livermore National Laboratory – [and] might have been able to predict the collapse of the buildings if anyone had considered the circumstances of a fuel-laden plan hitting the towers."[116] They cite as evidence the fact that "planes that struck the trade towers both came in with angled wings, suggesting that they were trying to knock out structural columns on as many floors as possible."[117]

But self-policing, or withholding scientific information, would likely be controversial within the research community since they conflict with traditional norms of scientific freedom. For instance, a U.S. scientist, Martin Hellman, developed unbreakable codes for encrypting data and communications and placed directions for their use by ordinary citizens on the Internet, despite the National Security Agency's (N.S.A) attempts to classify his work. Hellman and others contended that classifying this information would violate academic freedom and be an unwarranted limitation on their right to publish. But, reportedly, terrorists have used Hellman's codes to

---

[115]Steven Levy, "Tech's Double-Edged Sword: The Same Modern Tools That Enrich Our Lives Can Be Used Against Us. How Bad Will It Get?," *Newsweek*, Sept. 24, 2001, p. 65.

[116]James Glanz, "F.B.I. Studies Terrorists' Engineering Expertise," *New York Times*, Dec. 12, 2001.

[117]Glanz, Dec. 12, 2001. It was recently announced that a forthcoming report by the Federal Emergency Management Agency and the American Society of Civil Engineers concluded that there may have been no reasonable precautions that could have stopped the [World Trade] towers from collapsing once they were struck and huge fires broke out." (Eric Lipton and James Glanz, "U.S. Report on Trade Center Echoes Lessons of Past Disasters,"*New York Times*, Apr. 2, 2002.)

encrypt messages, rendering them impenetrable to intelligence services.[118] As another example, according to *New York Times* writer Gina Kolata, nanotechnology "could produce weapons with the power of a supercomputer embedded on the head of a bullet. ...It is a technology whose consequences could be so terrifying that one scientist, Dr. K. Eric Drexler, who saw what it could do, at first thought that he should never tell anyone what he was imagining for fear that those dreadful abuses might come to pass."[119]

Reportedly, scientists have engaged in self-policing in the past, for instance during the late 1930s when some scientists engaged in a "voluntary effort to withhold experimental data concerning nuclear fission...."[120] More recently, there have been numerous proposals for voluntary regulation or self-policing by scientists. For instance, it was reported in the press that Dr. Anthony Fauci, director of the NIH's National Institute of Allergy and Infectious Diseases (which funds most of NIH's research against bioterrrorism), and others agreed that "...biologists must become more aware of potential destructive applications of their work" and that scientific societies should take "...a lead in promoting debate" about this issue.[121] Dr. Raymond A. Zlinikas, a biological weapons expert at the Monterey Institute of International Studies, recommended that, in order to examine the need to withhold some biological sciences information, "... scientists should convene a meeting like the one at the Asilomar conference center in California in 1975, when scientists voluntarily adopted guidelines regulating what was then the new technology of genetic engineering."[122] John Steinbruner, director of the Center for International and Security Studies at the University of Maryland and vice-chair of the Committee on International Security and Arms Control of the National Academy of Sciences, proposed creating a "regime" to prevent "destructive applications of biotechnology research," which would be overseen by a global apparatus that would have responsibility for "identification of the investigators, registering of the principal investigators and their facilities; tracking the pathogens used in the research; peer review not only of the scientific but also of the social implications of the research; and legal specifications, such as how to protect proprietary property and security interests."[123] Similarly, George Poste, who chairs a Defense Department (DOD) task force on bioterrorism and is a member of the Defense Science Board, suggested that either more biotechnology work needs to be classified, or that biologists "must begin a process of self-regulation of projects that have potential applications in developing bioweapons...." His specific concerns focused on

---

[118]Gina Kolata, "When Science Inadvertently Aids An Enemy," *New York Times,* Sept. 26, 2001.

[119]Kolata, Sept. 26, 2001.

[120]Steven Aftergood, "Secrecy and Science," *Secrecy News*, Feb. 18, 2002.

[121]Peter Aldhous, "Biologists Urged to Address Risk of Data Aiding Bioweapons Design," *Nature,* Nov. 15, 2001, pp. 237-238.

[122]Andrew Pollack, "Scientists Ponder Limits on Access to Germ Research," *New York Times,* Nov. 27, 2001.

[123]Janet Aker, "Dangerous Biotech Research –Public and Private – Would Be Monitored by Proposed Global Oversight Body," *Washington Fax*, Dec. 12, 2001.

> projects in which viruses are engineered to evade or manipulate the immune system. For instance, earlier this year Australian researchers relate that they had inadvertently created a super-virulent strain of mousepox in a project aimed at creating a contraceptive vaccine. And gene therapists, grappling with the problems caused by immune reactions to the viral vectors they use to introduce therapeutic genes, are now designing 'stealth' vectors that would escape the attention of the immune system. Such technologies could be applied to viral bioweapons with devastating effects, argues Poste.[124]

Proposals for "Tiered" or Restricted Access to Information. Some experts propose that scientists should develop processes to categorize types of information in a research project or report and selectively disseminate restricted information only to qualified persons, or allow access to this information only on a need-to-know basis. For instance, Poste said that researchers should declare, when applying for a grant, whether the research could result in threatening applications, with the possibility of the sponsoring agency denying permission to publish; or, for example, that "anyone wishing to access genomic sequence data for dangerous pathogens might be required to provide evidence of their accreditation with a legitimate laboratory."[125] Reportedly "...the White House has asked the American Society of Microbiology...to limit potentially dangerous information in the 11 journals it publishes, including *Infection and Immunity, The Journal of Bacteriology,* and *The Journal of Virology*. One reported White House proposal is to eliminate the sections of articles that give experimental details researchers from other laboratories would need to replicate the claimed results, helping to prove their validity."[126] Others say restrictions should be placed on information about particular genes that cause a given microbe to be unusually deadly and that "[s]ome scientists have already abandoned certain research efforts, fearing the results could fall into the wrong hands."[127] For instance, Craig Venter at the Institute for Genomic Research said his firm halted a project on making artificial microbes. " 'We were going to make a synthetic micro-organism to study biology and evolution' but decided to stop since techniques could be used to make a synthetic pathogen."[128]

During the aforementioned National Academies' meeting in December on scientific openness at universities, Dr. Charles Vest, president of the Massachusetts Institute of Technology, proposed a taxonomy to evaluate the risks of open access to scientific information and materials. It included three categories of risk, ranging from "serious" to "more or less modest," to "minor or non-existent." He suggested distinguishing between scientific "know-how" and "fundamental information" to categorize risk. "Therefore, how to build a nuclear bomb belongs in the "serious" risk category, whereas basic physics belongs in the "minor or non-existent" risk

---

[124]Aldhous, Nov. 15, 2001.

[125]Aldhous, Nov.15, 2001.

[126]Broad, Feb. 17, 2002.

[127]Pollack, Nov. 27, 2001.

[128]Pollack, Nov. 27, 2001.

category."[129] It was reported in February that the Environmental Protection Agency (EPA) is trying to develop a plan to make information on chemicals available in a "tiered" manner, "such as making available less-detailed information, or making it available to a smaller, more limited group of people. ....For example, general information about facilities and chemicals would be available to everyone on EPA's site on the World Wide Web. A second tier of resources that would be more detailed would be available to users who 'want to register with the site, and let us know who you are.... A third set of resources would 'require more verification' from users...."[130]

Other agencies have taken actions to limit access to information. The Department of Transportation's Office of Pipeline Safety (OPS) has discontinued providing open access to the National Pipeline Mapping System (NPMS). Because of security concerns, "OPS no longer provides unlimited access to the Internet mapping application, pipeline data, and drinking water unusually sensitive area data." Access to data, but not to Internet mapping applications, is being provided only to pipeline operators and local, state, and federal government officials.[131] The Bureau of Transportation Statistics's (BTS) National Transportation Atlas Databases (NTAD) and North American Transportation Atlas (NORTAD), which provided geospatial data relevant to the National Pipeline Mapping System, have limited user access. Data will be provided, after consideration of a written request, only to Federal, state, and local government officials. BTS is reevaluating whether the data will be provided in the future.[132]

In opposition to some of these moves, critics say that the R&D that some seek to control is vastly different from the World War II Manhattan Project which isolated nuclear weapons scientists to conduct research at secret sites, making it easy to control their activities. Requiring scientists in specific fields to withhold basic research information until approval is received from some authority, they say, could seriously constrain scientific inquiry and scientific publication. They fear that rules to withhold information could be especially insidious, because, as expressed by a *New York Times* writer, "...the same tools, information, and experiments that would be used to develop weapons are used to make drugs as well." He gave an example,

> Some scientists are worried that the complete genome sequences of dozens of pathogens including the smallpox virus, are publicly available, giving weapon designers potential clues for ways to make pathogens worse. But the same information can also be used to help develop treatments or to use genetic fingerprinting to help trace the source of an attack.[133]

---

[129]*National Academies' Report on Post-September 11 Scientific Openness at Universities.*

[130]Hazardous Substances: Agency Considers New Ways to Make Data on Internet Site Available to Public," *Daily Report for Executives,* Feb. 22, 2002.

[131]National Pipeline Mapping System, [http://www.npms.rspa.dot.gov/data/npms_data_down.htm].

[132]BTS Data, [http://www.npms.rspa.dot.gov/data/bts_data.htm].

[133]Pollack, Nov. 27, 2001.

Some professional groups are responding to the information access issue. The Federation of American Scientists, which started a project 10 years ago to open up access to more governmental data, "decided after September 11 to remove from its website information about United States intelligence and nuclear weapons sites."[134] The National Academy of Sciences, in cooperation with the American Society for Microbiology, the FASEB, and others are beginning studies to support design of rules for scientists aimed at deterring terrorism.[135]

Removal of Information from Agency Websites

Since September 11, 2001, the Government has imposed increasingly rigorous controls on access to scientific and technical information that could be of potential value to terrorists. As already noted, initially agencies engaged in selective removal of information from agency websites. During March 2002, the executive branch issued formal requirements for agencies to withdraw sensitive information from websites and, in the future, to withhold government information characterized as "sensitive but unclassified."

Policies for Removal of Sensitive Scientific and Technical Information From Websites. Initially some agencies shut down or withdrew from their websites information they said could raise security concerns or could be useful to potential terrorists. There is no government inventory of sites that have been closed or materials withdrawn since September 11. Reportedly, the Commerce Department withdrew almost 7,000 documents.[136] The *OMB Watch* has posted a growing list of removed material, that is periodically updated, but it is not complete.[137]

The National Infrastructure Protection Center (NIPC), a joint government/private sector organization responsible for threat assessment, warnings, and response relating to attacks against critical infrastructure, located at the FBI headquarters, issued a warning on January 17, 2002 to advise users that any information posted on the Internet could reach an "unintended" audience and pose a security hazard. It offered seven anti-terrorism related factors that administrators should consider when weighing the potential hazards and benefits of posting information related to critical infrastructures. The seven points are:

1. Has the information been cleared and authorized for public release?
2. Does the information provide details concerning enterprise safety and security? Are there alternative means of delivering sensitive security information to the intended audience?

---

[134]David E. Rosenbaum, "Breaking Law or Principles to Give Information to U.S.," *New York Times*, Nov. 23, 2001.

[135]Pollack, Nov. 27, 2001; Conversation with National Research Council staff member, Anne-Marie Mazza, Mar. 2002..

[136]William J. Broad, "U.S. Is Tightening Rules on Keeping Scientific Secrets," *New York Times*, Feb. 17, 200-2, pp. 1, 19.

[137]*OMB Watch*, "The Post-September 11 Environment: Access to Government Information." [http://www.ombwatch.org/info/2001/access.html].

3. Is any personal data posted (such as biographical data, addresses, etc.)?
4. How could someone intent on causing harm misuse this information?
5. Could this information be dangerous if it were used in conjunction with other publicly available data?
6. Could someone use the information to target your personnel or resources?
7. Many archival sites exist on the Internet, and that information removed from an official site might nevertheless remain publicly available elsewhere.[138]

Many experts have applauded these moves as an effective way to withhold sensitive information about vulnerabilities in infrastructure or about science and technology information that could be used to make weapons. But some question whether legitimate scientists and the public will be able to gain access to information they need to conduct R&D or to participate in public processes relating to regulation, industrial pollution or environmental action – processes that remain open to public scrutiny. Furthermore, some say that much of the removed information is still available in cached Internet sites. In most cases when an agency removed data from its website it "posted notices that the information had been removed because of its possible usefulness to terrorists."[139]

Illustrations of Information That Was Removed. Among the agencies removing restricting information were the Environmental Protection Agency, the Department of Energy and related agencies, and other agencies.

Environmental Protection Agency. In March 2002, the Environmental Protection Agency (EPA) decided to restrict access to its "Envirofacts" database website. Previously, researchers and the public were able to download manipulable databases that contain information on multiple sites for chemical releases, toxic waste, and so forth. Now researchers will be able to access data only on one facility at a time. Multiple site data are available only to "EPA employees, EPA contractors, the military, federal government, and state agency employees," according to EPA. A researcher at the University of Michigan's School of Natural Resources and Environment, said "this will 'basically make our research impossible'...."[140] Apparently EPA is attempting to find alternatives to meet their needs and to help researchers find alternative access.

The EPA National Exposure Research laboratory website was closed pending a review of its contents. The site, which is used by toxicologists and the public, includes information about chemical facilities and the risks posed to people and the environment by spills from chemical plants. (EPA is required to provide public access to information about environmental releases of chemicals under The Emergency

---

[138]NIPC, "Internet Content Advisory: Considering the Unintended Audience," Jan. 17, 2002, Advisory 02-001 [http://www.nipc.gov/warnings/advisories/2002/02-001.htm].

[139]"Freedom of Information Act," in *Homefront Confidential,* March 2002, p. 25. For additional information, see Reporters Committee for Freedom of the Press, "Freedom on Information," *Homefront Confidential. How the War on Terrorism Affects Access to Information and the Public's Right to Know,* RCFP White Paper, March 2002, pp. 21-27.

[140]Meredith Preston, "Researcher Says Work May Be Impeded By Restrictions on Environmental Database," *Daily Report for Executives,* Mar. 28, 2002.

Planning and Community Right-to-Know Act (EPCRA, codified at 42 U.S.C. 11001-11050), enacted in 1986 as Title III of the Superfund Amendments and Reauthorization Act (P.L. 99-499).[141] Access to such data has long been controversial. Proponents of open access contend it is necessary for emergency planning (such as for firefighters to evaluate risks) and for pollution control monitoring. Objectors cite the costs of providing the data, suggest that it could serve terrorists, and fear that the information could unduly frighten residents who live near chemical facilities. The chemical industry has also sought to limit some of this information. It has been reported that "[T]he American Chemistry Council, the trade association for chemical manufacturers, and other trade associations, such as the American Water Works Association, have lobbied for years to limit or shut down public access to information about hazardous chemicals being used in the community, including through public reading rooms –and now justify removal with the threat of terrorism."[142] In addition, representatives of the chemical industry reportedly asked EPA temporarily, pending review, to curtail public access to "50 off-site reading rooms for access to computerized information describing worst-case scenarios in possible accidents at chemical plants."[143]

Department of Energy and Related Agencies. The Department of Energy (DOE) removed sensitive maps and descriptions of ten governmental nuclear facilities with weapons-grade plutonium and highly-enriched uranium after it was alerted to the public's ability to access these sites by the Project on Government Oversight (POGO), which traditionally objects to governmental restrictions on government information.[144] Reportedly, much of this information is still available online from other sources.[145] The Nuclear Regulatory Commission shut down its website after the September 11 attacks, and, when it reopened, did not include formerly posted information about Nuclear Reactors, Operating Reactors, Generic Environmental Impact Statements for License Renewal of Nuclear Plants, Nuclear Materials, and Radioactive Waste[146]

After the fall 2001 terrorist attacks, the Federal Energy Regulatory Commission (FERC), part of the Department of Energy, issued a policy statement "removing from easy public access previously public documents that detail the specifications of energy facilities licensed or certificated by the Commission." On January 16, 2002, FERC

---

[141]For additional information see, "Emergency Planning and Community Right-to-Know act," by Linda Schierow, in *Environmental Laws: Summaries of Statutes administered by the Environmental Protection Agency*, coordinated by Martin R. Lee, Jan. 4, 2001, pp. 80-85.

[142]"Right-to Know Public Access to Government Information," *OMB Watch*, Feb. 19, 2002.

[143]Meredith Preston, "Chemical Industry Urges Restriction on Access to Worst-Case Scenario Data," *Daily Report for Executives*, Oct. 9, 2001, p. A-25.

[144]"POGO Supports the DOE's Removal of Sensitiva Documents From Its Website," Project on Government Oversight, Press Release, Nov. 8, 2001, [http://www.pogo.org/nuclear/security/doeweb.htm].

[145]Joshua Dean, "Energy Pulls Sensitive Nuclear Information From the Web," *GovExec.com*, Nov. 12, 2001.

[146][http://www.nrc.gov/].

published in the *Federal Register* a notice that it was soliciting information from the public to "assist the Commission in determining what changes, if any, should be made to its regulations to restrict unfettered general public access to critical energy infrastructure information, but still permit those with a need for the information to obtain it in an efficient manner." Comments were due by March 1, 2002.[147]

It was announced on December 16, 2001, that the Defense Nuclear Facilities Safety Board (DNFSB), an independent U.S. Government agency charged with oversight of U.S. Department of Energy nuclear safety issues, halted all public access to technical documents it had obtained from the DOE. The DNFSB also stopped providing printouts of documents in its possession.[148]

Other Agencies. The National Imagery and Mapping Agency (NIMA), which removed maps from its own website, reportedly directed the U.S. Geological Survey and the Federal Aviation Administration (FAA) to halt sales of all NIMA-made topographic maps, and ordered the Library of Congress and the National Archives and Records Administration to deny pubic access to such maps.[149] In addition, the Superintendent of Documents requested in October 2001 that federal depository libraries (reportedly 335 mostly academic libraries)[150] to withdraw from public circulation, and destroy, their depository copies of a U.S. Geological Survey CD-ROM[151] providing information about large public water resources because it contained sensitive information. Technically depository documents are the property of the U.S. government. The U.S. Government Printing Office (GPO) reported that this was the only CD-ROM that it asked depository libraries to remove.[152]

Reportedly, the Centers for Disease Control and Prevention (CDC) withdrew a report on lack of preparedness against a terrorist attack using poison gas or other chemical agents.[153]

The U.S. government also has taken steps to limit access to satellite data which could prove to be a security threat or advantageous to terrorists. For instance, the *New York Times* reported that the government bought exclusive rights to images of

---

[147]*Federal Register,* Jan. 23, 2002, p. 3129-3135.

[148]"Public Faces Further, Unexplained Restriction in Access to Information - Defense Nuclear Facilities Safety Board Instructed to Slap Lid on DOE Documents," Dec. 16, 2001, Released by the Federation of American Scientists at (http://www.fas.org/sgp/news/2001/12/clements.html].

[149][http://WWW.GOVexec.com/dailyfed/0901/092501p1.htm].

[150]Alex P. Kellogg, "An Order to Destroy a CD-ROM Raises Concerns among University Librarians," *Chronicle of Higher Education,* Feb. 14, 2002.

[151]Entitled "Source-Area Characteristics of Large Public Surface Water Supplies in the conterminous United States: An Information Resource for Source-Water Assessment, 1999," according to Kellogg, Feb. 14, 2002.

[152]"Statement on Request to Withdraw USGS Source-Water CD-ROM From Depository Libraries," *U.S. GPO News Release 02-04,* Jan. 16, 2002.

[153]"Intelligence Data Pulled From Websites," *BBC News* website, Oct. 5, 2001.

Afghanistan and parts of surrounding nations that are taken by *Ikonos*, a US. commercial imaging satellite. The newspaper wrote, "The National Imagery and Mapping Agency said it paid $1.91 million for the first 30 days of the contract, which went into effect on Oct. 7, the day U.S.-led air strikes began. It gives the U.S. military 'assured access' to images collected by the company's IKONOS satellite." While the imagery reportedly has helped the military plan air strikes,[154] some say that the government's main motivation "... is to prevent images of civilian targets hit during bombing raids reaching the media."[155] The U.S. government apparently has the authority also has the ability to restrict access to commercial satellite images through the courts in times of war.[156]

Classification of Scientific and Technical Information

Introduction to the Issue. Most basic and academic scientific research supported by the government has not been classified. (This topic is discussed in more detail in the next section.) But, reportedly, OSTP director John Marburger and other officials "have suggested that homeland security may require academic scientists to withhold the fruits of some research, such as the genetic sequences of potential bioweapons or the recipes for toxic chemicals."[157] This is a controversial issue since some researchers may be forced to accept classified research to obtain funds.[158] Some universities are reviewing their decisions not to allow classified research activities on campus. Consideration is being given to allow agencies to reclassify already released materials and to permit some agencies, such as the National Institutes of Health, that formerly did not classify information, to do so. In addition, the White House has issued a government-wide policy to restrict release of "sensitive but unclassified" information. "Sensitive" is not defined.

Actions Taken Regarding Classification and Reclassification. While national security agencies still have wide powers to classify information, because of steps taken by President Bill Clinton to open access to formally classified materials,[159] the trend had been toward less classification and secrecy in recent years. This trend may be changing. The Bush Administration is seeking to halt the distribution and sale of government documents that explain how to develop biological weapons that were declassified and are available from agencies for sale or via FOIA requests. Such documents were written from 1943 to 1969 when the United States researched, developed, and built a stockpile of biological weapons. Reportedly, the

---

[154]U.S. in Talks to Keeps Rights to Satellite Images," *New York Times*, Oct. 30, 2001.

[155]James Randerson, *New Scientist Online News*, Oct. 17, 2001.

[156]Randerson, op. cit.

[157]Check, Feb. 21, 2002, Aftergood, Feb. 28, 2002

[158]Check, Feb. 21, 2002, Aftergood, Feb. 28, 2002.

[159]Executive Order 12958, "Classified National Security Information."

Administration has closed public access to over 6,600 technical government reports dealing with biological and chemical weapons production.[160]

On December 12, 2001, President Bush granted the Secretary of the Department of of Health and Human Services, which traditionally does not classify information, power to classify information as secret.[161] According to an agency spokesperson, the documents to be classified include those relating to bioterrorism and the nation's preparedness to respond to it. "Officials said the kind of information that might be classified would be storage sites for vaccine stockpiles, certain laboratory floor plans or some details about emergency medical stocks."[162] In response, an official with the American Society for Microbiology (ASM), reported that "...that the society is concerned about the implementation of an order signed last October by President Bush allowing the health department — including the NIH — to fund classified projects."[163]

Reclassification of already released information is also an important issue. Previous administrations had from time to time reclassified information, but each had a different policy. Until March of 2002, reclassification of already released, formerly classified information was permitted only if the information had not been officially released to the public.[164] Several executive office groups examined the pros and cons of reclassification. The Office of Science and Technology Policy (OSTP) examined whether an executive order should be issued permitting reclassification or whether

---

[160]William J. Broad, "U.S. Tightening Rules on Keeping Scientific Secrets,: *New York Times*, Feb. 17, 2002.

[161]Alison Mitchell, "A Nation Challenged: Classified Information; Bush Gives Secrecy Power to Public Health Secretary," *New York Times*, Dec. 20, 2001.

[162] Mitchell, op. cit.

[163]Erika Check, "Biologists Apprehensive Over US Moves to Censor Information Flow," *Nature*, Feb. 21, 2002.

[164]"The question of whether documents, once declassified, can be or should be reclassified has been asked on a number of occasions over the years, and then answered in different ways. Nuclear weapons information, once declassified, cannot be reclassified, according to the Department of Energy's interpretation of Section 142 of the Atomic Energy Act of 1954 (42 U.S.C. 2162). (DOE officials sometimes finagle this restriction by withholding the declassified information as Unclassified Controlled Nuclear Information.) Under President Reagan, officials were permitted to reclassify declassified information and documents under certain conditions. This authority was exercised on numerous occasions, but these do not seem to have been publicly reported. See Section 1.6(c) and (d) of President Reagan's Executive Order 12356: [http://www.fas.org/irp/offdocs/eo12356.htm#reclass]. President Clinton permitted reclassification of declassified information only if it had not been officially released to the public. Once it was officially released it could not then be reclassified. See Section 1.8(c) and (d) of President Clinton's Executive Order 12958, which remains in effect today: [http://www.fas.org/sgp/clinton/eo12958.html#reclass]. A review of this executive order is now underway by the Bush Administration and may include consideration of expanded authority to reclassify declassified information." ("Reclassifying Declassified Documents," *Secrecy News from the FAS Project on Government Secrecy*, Jan. 15, 2002.)

distribution could or should be halted even with FOIA requests for this information.[165] Reportedly, the Defense Technical Information Center (DTIC) "said panels of scientific experts would be assembled to see whether the [aforementioned bioweapons] documents should once again be made available to the public or perhaps reclassified as state secrets."[166] The National Academy of Sciences started to develop panels to deal with these issues.[167] The Federation of American Scientists (FAS) urged that "any such reclassification authority be narrowly circumscribed and that agency proposals for reclassification actions be subject to independent approval or rejection by the Interagency Security Classification Appeals Panel."[168]

On March 18, 2002, White House Chief of Staff Andrew H. Card, Jr., issued a memorandum for the heads of Executive Departments and Agencies to not "disclose inappropriately" government information regardless of age relating to weapons of mass destruction, defined to include chemical, biological, radiological, and nuclear weapons "as well as other information that could be misused to harm the security of our Nation and the safety of our people."[169] Agencies were given guidance, prepared by the Department of Justice, to identify appropriate documents and records, and were asked to report within 90 days to the President's Chief of Staff and the Office of Homeland Security on actions taken.[170] The guidance issued on March 18 also called for reclassification of formerly classified sensitive information. It also stated "The need to protect such sensitive information ["related to America's homeland security"] from inappropriate disclosure should be carefully considered, on a case-by-case basis, together with the benefits that result from the open and efficient exchange of scientific, technical, and like information."[171] "Sensitive" was not defined. The memo also applies to information that would be released via FOIA requests. Some observers believe this could lead to removal of considerably more documents from agency websites and has led to concerns among advocates for open government about the "sensitive but unclassified information" category[172] and among scientists, even

---

[165] William J. Broad, "U.S. Is Still Selling Reports on Making Biological Weapons," *New York Times*, Jan 13, 2002.

[166]Broad, Feb. 17, 2002.

[167]Broad, Feb. 17, 2002.

[168]"Reclassifying Declassified Documents," op. cit.

[169]Memorandum entitled "Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security," Mar. 19, 2002.

[170]Information Security Oversight Office, National Archives and Records Administration, and Department of Justice, "Memorandum "Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security," Mar. 19, 2002. [http://www.fas.org/sgp/bush/who31902/html].

[171]Information Security Oversight Office, National Archives and Records Administration, and Department of Justice, "Memorandum "Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security," Mar. 19, 2002.

[172]"Government Puts New Controls on Public Access to Weapons Info.," *The Mercury News*, Mar. 21, 2002.

though the memo called for balance in safeguarding scientific and technical information.[173]

Similar kinds of security measures are being taken in Great Britain. For example, some British researchers are complaining that new export control laws under consideration in the United Kingdom that would prohibit the export of information, "will in theory allow government vetting of scientific material before publication."[174] The bill would "authorize government scrutiny of the 'intangibles' researchers might be transferring, through publishing or teaching, to foreign powers" and it "would govern internal communications, "meaning any scientists submitting research for publication in a British journal would be subjected to the controls."[175] Apparently, many British researchers seek to modify the legislation to exclude basic research.

Some Universities Are Considering Allowing Classified Research to Be Conducted On-campus. Most research universities have prohibited the conduct of classified research on campus as detrimental to teaching and scholarship, and permit such research to be conducted only in affiliated off-campus fenced research laboratories which typically are off-limits to foreign students and researchers.[176] Sometimes universities allow on-campus researchers supported by industrial firms and contracts to restrict publication of research results until after release by the industrial sponsor. Apparently some university officials, for instance at the Massachusetts Institute of Technology, Stanford University, the State University of New York, and other schools, have started to review policies toward classification in the interest of better serving the nation's anti-terrorist efforts. [177]

Federal policy regarding classified university research seems imprecise. Traditionally, federally-funded research by extramural and many intramural performers, even in the defense area, has not been classified.[178] Nevertheless, it has been reported that some researchers feel the pressure of subtle government moves to control research results even in the absence of classification rules. "The Pentagon currently imposes no limits on basic research that it funds and seeks review only of applied science projects. But 'it's a policy with nuance,' says...an administrator at Johns Hopkins University's applied Physics Laboratory.... 'As a practical matter, some investigators are urged by [military] sponsors to delay or withhold basic

---

[173]Bill Sammon, "Web Sites Told to Delete Data," *The Washington Times,* Mar. 21, 2002.

[174]Check, Feb. 21. 2002. See also Kate Galbraith, "British Scientists Fear That 'Export Control Bill' Could Strangle Research," *Chronicle of Higher Education,* Feb. 20, 2002.

[175]John T. Softcheck, "U.K. Scientists Fear 'Academic Censorship' Provisions in Export Control Bill," *Washington Fax,* Feb. 22, 2002.

[176]Steven Aftergood, "Controversy Over Classified Research on Campus," *Secrecy News,* Feb. 28, 2002.

[177]Aftergood, Feb. 28, 2002. See also: "New Committee to Look At Institute Policies on Scientific Information Access, Disclosure," *MIT Tech Talk,* Feb. 13, 2002.

[178]Discussed in *Report of the Defense Science Board Task Force on Secrecy,* July 1970, as described in Aftergood, Feb, 18, 2002.

research results, ...[and] universities are kidding themselves if they think all faculty will adhere to an academic policy that is not in their best interests."[179]

Expanding Exemptions To the Freedom of Information Act

The Freedom of Information Act (5 U.S.C. 552), enacted in 1966 and subsequently amended, establishes for any person – corporate or individual, regardless of nationality – presumptive access to existing, unpublished agency records on any topic. The law specifies nine categories of information that may be exempted permissibly from the rule of disclosure. Certain kinds of proprietary or trade information are protected from disclosure. However, the existing "exemptions do not require agencies to withhold information, but merely permit access restriction."[180] Disputes over the accessibility of requested records may be settled in federal court. Fees for search, review, or copying of materials may be imposed; also, for some types of requesters, fees may be reduced or waived. The act was amended in 1996 to provide for public access to information in an electronic form or format.[181]

Arguments have been made that to enhance counter terrorism, the exemptions to disclosure under FOIA should be extended to include certain information about infrastructures and research and development. It has been argued that in order to protect certain infrastructures against terrorists, private companies would have to divulge certain information to the government, and that unless this information were exempt from disclosure under FOIA, the private sector would not cooperate in providing information about certain infrastructures and their potential vulnerabilities (power plants, chemical plants, and so forth). Richard Clarke, the President's computer security adviser and chair of the President's Critical Infrastructure Protection Board set up under the Office of Homeland Security, addressed this topic in relation to information technology infrastructure. He suggested to attendees at the Business Software Alliance's Global Tech Summit that, "Congress could encourage the private sector to cooperate with the government by exempting necessary disclosures from the Freedom of Information Act, so that information about security weaknesses would not get into the public's hands."[182]

Several legislative proposals relating to research and development for counter terrorism would exempt certain R&D-related information from disclosure under the Freedom of Information Act. S. 1456, the "Critical Infrastructure Information Security Act of 2001," would provide exemptions from disclosure under FOIA for information related to industrial cybersecurity and critical infrastructure "that is

---

[179]David Malakoff, "Universities Review Policies for Onsite Classified Research," *Science,* Feb. 22, 2002.

[180]*The Administration and Operation of the Freedom of Information Act: An Overview, 1966-1991,* by Harold C. Relyea, CRS report 93-977, Nov. 4, 1993.

[181]*Access to Government Information in the United States,* by Harold C. Relyea, CRS Report 97-71, June 28, 2001, 4 p.

[182]Anandashankar Mazumdar, "Computer Security: Administration Point Man on Cybersecurity Says Private Sector Aid Essential to Security," *Daily Report for Executives,* Dec. 5, 2001, p. A-15.

voluntarily submitted to specified Federal agencies for analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose...." H.R. 2435, the "Cyber Security Information Act" provides that (with exceptions) "any information voluntarily provided directly to the government about a firm's cyber security, a third party's cyber security, or to an Information Sharing Organization which is subsequently provided to the Government in identifiable form shall: (1) be exempt from disclosure under the Freedom of Information Act; (2) not be disclosed to any third party; and (3) not be used by any Federal or state entity or by any third party in any civil action."

As noted above, two similar bills on bioterrorism – S. 1765, passed in the Senate (as a substitute amendment for H.R. 3448), and H.R. 3448, passed in the House – would exempt from disclosure under FOIA information about the locations and quantities of certain biological agents and toxins held by laboratories, including private sector laboratories. Certain kinds of biological information would be protected from disclosure under FOIA in H.R. 3160, the Bioterrorism Prevention Act of 2001.

The executive branch has also taken action regarding access to information under FOIA. First, on October 12, 2001, Attorney General John Ashcroft issued a memorandum to federal agencies urging them to exercise caution in disclosing information requested under FOIA in order to help protect the nation against terrorism. *OMB Watch* writers concluded that "the new message from the Attorney General to the agencies is to, where possible, withhold the information from disclosure. This is a fundamental reversal of past policies that emphasized, where possible, to disclose the information."[183] Specifically,

> The memo affirms the Justice Department's commitment to "full compliance with the Freedom of Information Act," but then immediately states it is "equally committed to protecting other fundamental values that are held by our society. Among them are safeguarding our national security, enhancing the effectiveness of our law enforcement agencies, protecting sensitive business information and, not least, preserving personal privacy."
>
> This new policy supersedes a 1993 memorandum from then-Attorney General Janet Reno that promoted disclosure of government information under FOIA unless it was "reasonably foreseeable that disclosure would be harmful." This standard of "foreseeable harm" is dropped in the Ashcroft memo. Instead, Ashcroft advises, "When you carefully consider FOIA requests and decide to withhold records, in whole or in part, you can be assured that the Department of Justice will defend your decisions unless they lack a sound legal basis..."[184]

Second, as noted already, the Card memorandum of March 18, 2002, which says it specifically applies to information requested to be released under FOIA, requests that agencies not "disclose inappropriately" government information regardless of age

---

[183]"Right-to-Know: Public Access to Government Information," *OMB Watch*, 2/19/02.

[184]For additional information, see Reporters Committee for Freedom of the Press, "Freedom on Information," *Homefront Confidential. How the War on Terrorism Affects Access to Information and the Public's Right to Know*, RCFP White Paper, March 2002, pp. 21-27.

relating to weapons of mass destruction defined to include chemical, biological, radiological, and nuclear weapons "as well as other information that could be misused to harm the security of our Nation and the safety of our people."

Implications

Self-policing, withdrawing already released scientific and technical information, or classifying certain information are intended to prevent potential terrorists from gaining access to detailed scientific and technical data which could be used to harm the United States, or information on infrastructure sites and their vulnerabilities to attack. Reaching a balance between openness and secrecy in access to scientific and technical information remains a contentious issue.

One major argument made against restricting access to scientific and technical information is that it "could make it impossible for scientists to assess and replicate the work of their colleagues, eroding the foundations of American science. ...[Some scientists]...fear that government officials eager for the protections of secrecy will overlook how open research on dangerous substances can produce a wealth of cures, disease antidotes and surprise discoveries."[185] Robert R. Rich, President of the Federation of American Societies for Experimental Biology, expressed his judgment: " 'I think the risk of forgone advances is much greater than the information getting into the wrong hands,' "[186] he added. " 'There is very little that comes out of university labs that could conceivably be considered sensitive,' he said. "So to set up any kind of blanket policy that would require general pre-review of scientific publications would be extraordinarily cost-ineffective and would stifle the communication of important research findings.' "[187]

Some critics believe that withholding scientific and technical information will not deter terrorists. They say that a lot of the withdrawn materials are still available to the public via cached sites on Internet search engines[188] or in hard copy at depository libraries. Others argue that the prevention of terrorism requires openness in scientific information in order to foster a reciprocal worldwide response. For instance, some arms control advocates object to these provisions. " 'Instead of promoting secrecy on biological weapons research, to restore international confidence in biological weapons control, the US should be moving in the opposite direction to promote high transparency,' declared the Sunshine Project, a watchdog group."[189]

Some are concerned that national security will be used as a pretext to keep information from the public, and that public access will be curtailed to important

---

[185]Broad, Feb. 17, 2002.

[186]Broad, Feb. 17, 2002.

[187]Broad, Feb. 17, 2002.

[188]"U.S. Websites Closed in Anti-Terrorist Bid," *Nature, News in Brief*, Oct. 11, 2001.

[189]See the Project's "Seven Good Reasons to Stand Up for Information Freedom on Bioweapons Research," [http://www.sunshine-project.org/publications/pr301001.html], cited in *Secrecy News*, from the FAS Project on Government Secrecy, Nov. 28, 2001.

information needed to critique regulations, provide for public discussion, and so forth.[190] For instance, specific objections have been raised by critics at a public group called the Nuclear Control Institute. Regarding the withdrawal of information from the Defense Nuclear Facilities Safety Board website, they said, "Slamming this window shut under the guise of national security could well prove to be a disservice to those working in the public interest on [Department of Energy] DOE issues. DOE should take immediate action to clarify release of technical documents in the hands of the DNSFB and pledge only to withhold information which could clearly benefit someone with malevolent intent."[191] With respect to the bills that would exempt from FOIA cybersecurity and critical infrastructure information, it has been reported that, "Groups that advocate open records, environmentalists, and others allege that ...[some proposed...] legislation 'would profoundly undermine the ability of the Environmental Protection Agency to sue polluters.' "[192] For example, the Children's Environmental Health Network (CEHN) and other groups opposed the EPA's decision to remove information from its website regarding chemical industries' emergency response plans. They argued that well-trained terrorists would get the withheld information anyway, and that there should be "public discussions held on the public's right to know and if limits should be placed on that information." In a letter sent to the White House and the Department of Justice, the coalition said that the public needs information on hazardous conditions to make informed choices and decisions and to enable health practitioners to treat environmental exposures and to ensure that industries implement appropriate safety measures. [193]

Agencies are required to report to the Office of Homeland Security and the White House over the next three months about steps they have taken to safeguard "sensitive" information released in the past and plans for the future, and some agencies have been given new classification authority. Some agencies are developing guidelines for "tiering" or categorizing certain kinds of information to allow for restricted access to those with a need for the information, including researchers in some cases. The National Academy of Sciences is working with professional associations to examine self-policing by scientists themselves. The public and members of the scientific community may examine these activities and try to influence the development of rules that they believe balance securing the nation against terrorism and providing for their particular requirements.

---

[190]See "Benefits of Chemical Information Should Not be Forgotten," *OMB Watch*, [http://www.ombwatch.org/execreport/remp.html].

[191]"Public Faces Further, Unexplained Restriction in Access to Information - Defense Nuclear Facilities Safety Board Instructed to Slap Lid on DOE Documents," Dec. 16, 2001 [http://www.fas.org/sgp/news/2001/12/clements.html].

[192]Drew Clark, "Environmental Groups Protect Cybersecurity Information Sharing Bill," *Gov.Exec. com*, Dec. 3, 2001.

[193]"Hazardous Substances Coalition Says Response to Terrorism Should Not Limit Access to Information," *Daily Report for Executives*, Nov. 8, 2001, p. A-46.

Export Controls

Since the September 11th attacks, the U.S. Government has taken action to tighten exports of sensitive technologies to potential terrorists. On December 10, 2001, the U.S. Customs Commissioner announced the launch of "Operation Shield America," which seeks to increase the list of items on existing State Department and Commerce Department export control lists that might be of potential interest to international terrorist organizations, that would be subject to surveillance, and could not be exported freely. The activity also involves providing U.S. companies with instructions about how to spot suspicious buyers. "Customs has already taken key steps under this initiative. The Customs Intelligence Division has compiled a list of key technologies and weapons likely to be of interest to terrorist groups [and]... has shared this list with the intelligence community and with the Departments of State, Commerce, Defense, Energy, Treasury, and Justice. Customs is soliciting feedback from each in order to reach an accord on the items that should be the focus of Shield America." The list remains secret. The program is being implemented by federal agents canvassing U.S. manufactures of the items on the list "to educate about the program and encourage them to turn over names and information on any suspicious customers."[194] According to the Customs Service, "While some of these materials may seem relatively innocuous and have relatively little monetary value, they can have enormous strategic value in the hands of America's adversaries. These 'minor' technological goods could easily become the necessary component for major weapons development by terrorist groups or rogue nations." Continuing, Customs said

> In one particular case, for example, Customs investigated the export of a chemical called thiodiglycol. This chemical has civilian applications in the production of dyes and inks. However, thiodiglycol is also a key precursor in the production of mustard gas. The Customs investigation dismantled networks that were buying hundreds of tons of this material from a Baltimore firm and providing the chemical to Iran for use in mustard gas.
>
> > Several Customs investigations have disclosed illicit exports of high-speed timing devices known as "krytrons." While these devices have broad civilian applications in photocopiers and lasers, krytrons are also ideal for use in triggering nuclear warheads. In one noteworthy case, Customs intercepted 40 krytrons destined for an Iraqi military establishment after being purchased from a California firm.
>
> Because U.S. technology, munitions, and other equipment are among the highest quality in the world, foreign nations and others continuously target them for acquisition. According to a Sept. 2001 report by the Defense Security Service (DSS), individuals linked to no fewer than 63 nations were involved in "suspicious" efforts to obtain U.S. technology with military applications during

---

[194] Brock N. Meeks, "Terrorism 'Shopping List' Targeted," *MSNBC,* Dec. 10, 2002. See also, "U.S. Customs' "Operation Shield America," *Expeditors Newsflash*, Dec. 12, 2002, #250.

2000. The year before, the DSS reported that individuals tied to 56 nations were involved in efforts to acquire U.S. technology with military applications.[195]

Under the program, Customs says it doesn't want companies to investigate their clients, but the Customs Service will send agents to visit firms that manufacture or sell items on the list and ask companies to report suspicious behavior, such as "first-time customers who ask to pay for larger orders in cash or offer more than the market price."[196]

Implications

The major implication of these actions is the need to strike a balance between security and the competitiveness of commerce in science and technology. While controls on export of products that could be used to develop weapons against the United States are necessary, the unintended consequences of this action could jeopardize some U.S. foreign trade "because the list reportedly includes 'just about everything that you can imagine that relates to the production of any kind of weapon of mass destruction, whether that's a chemical weapon, a biological weapon, or nuclear weapon....' "[197] One observer commented that it is possible that the regulation could "stigmatize companies that directly or inadvertently sell to a terrorist since the program provides for voluntary compliance to "spot suspicious buyers."[198] Some worry about confusion in the proliferation of export controls and "denied persons" lists by various agencies and that "legitimate deals may be stonewalled while exporters are shunted back and forth" among agencies that have jurisdiction to withhold export licenses.[199] The government may need to monitor for effectiveness and impacts, the actions taken to collaborate with industry and to control exports

Activities of Scientific and Technical Professional Groups

Science and technology professional associations have organized groups and planned studies on counter terrorism in an effort to assist the government but also to position their members to monitor federal security actions and to track the availability of R&D funding opportunities. A few illustrative activities are described next. (See also CRS Report RL31202.)

---

[195]U.S. Customs Service, "U.S. Customs Launches 'Operation Shield America' New Initiative Seeks to Prevent Terrorist Organizations From Acquiring Sensitive U.S. Technology, Weapons, and Equipment," *Press Release,* Dec. 10, 2001.

[196]"Customs Dept. Deals With Technology," *AP* OnLine, Dec. 10, 2001.

[197]Rossella Brevetti, "Customs, Bonner Unveils Plan to Stop Terrorists From Acquiring Sensitive Technologies," *Daily Report for Executives,* December 12, 2001, p. A-16.

[198]Brevetti, op. cit.

[199]"Export ABCs: Security and Forwarders," Journal of Commerce Online, Jan. 28, 2002.

The National Academies

The National Academies – the Academy of Science, the Academy of Engineering, and the Institute of Medicine – are undertaking contract studies on specific topics for federal agencies through their research arm, the National Research Council. In addition the Academies established the Committee on the Science and Technology Agenda for Countering Terrorism, co-chaired by Lewis Branscomb, a Harvard professor, and Richard Klauser, former director of the National Cancer Institute. The committee consists of 22 leading nongovernmental scientists and technologists. Under Phase I of the project, the group will divide into panels in the areas of biological; chemical; nuclear and radiological R&D; information technology, computers, and telecommunications; transportation; energy facilities, buildings and fixed infrastructure; and behavioral, social and institutional issues. The groups will attempt to characterize the threat for each area, develop long-term research agendas and examine cross-cutting multidisciplinary research topics for these "domains," and conduct short-term studies and provide advice.[200] A research agenda for each of the seven target areas is to be produced by May 2002. The second phase will be a report that will focus on the organization of federal R&D agencies for counter terrorism. This report is expected by September 2002.[201] In addition, the National Academy of Engineering is planning a study of "homeland defense against terrorism."

Professional Associations

The American Association or the Advancement of Science held a symposium on December 18, 2001 on the topic of "The War on Terrorism: What Does It Mean for Science?"[202] The speakers, who included the OSTP Director, the president of the National Academy of Engineering, and several academic experts, focused on the proposed restructuring of the federal government to respond to terrorism, the impact of new security measures and terrorism initiatives on science, the impact of new visa and surveillance rules on students at U.S. universities, the responsibilities of scientists and engineers to contribute to national security and principles of conduct that should guide scientists and engineering in their work on issues that pose potentially high risk to human life.

The American Chemical Society, in cooperation with other professional associations,[203] through its *Vulnerability and Security* series, provides occasional

---

[200]"Klauser Accepts Position as National Academies' Adviser on Counter Terrorism," *National Academies News,* Dec. 19, 2001 and information about Project Number DEPS-L-01-02-A.

[201]Wil Lepkowski, "The Academies and the World," *Science and Policy Perspectives,* Dec. 11, 2001.

[202]Audio of the conference is available at: [http://www.aaas.org/spp/scifree/terrorism/].

[203] American Association of Engineering Societies, American Chemical Society, American Institute of Chemical Engineers, American Society of Civil Engineers, American Society of Mechanical Engineers, Council for Chemical Research, IEEE-USA Society for Risk Analysis,

(continued...)

briefings to Members of Congress and staff from experts on science and technology-related terrorism issues. Briefings have focused on nuclear infrastructure, chemical site security, chemical and biological terrorism.

The American Society of Civil Engineers wrote to OHS Director Tom Ridge on November 1, 2001, describing the society's civilian engineering study teams on disaster response procedure and a new Building Performance Study Team, created to gather data on the damage to the World Trade Center buildings and the Pentagon. It also described a study it was undertaking on critical infrastructure response and offered its assistance in generating legislative initiatives.[204]

The American Psychological Association (APA), created a Subcommittee on "Psychology's Response to Terrorism" that is developing an inventory of what psychologists can contribute to the efforts to address the threat as well as the impact of terrorism.[205] Among other things, it is assembling lists of psychologists who have worked on issues such as malignant attitude formation, peace psychology, conflict resolution, military psychology, and so forth and offering its services to the government. It is also developing materials and posting on the APA website materials dealing with the impact of terrorism, stress, and anxiety management support.[206]

Concluding Observations

A broad gamut of counter terrorism security measures have been adopted and proposed by the Congress, the President, and scientific and technical professional groups for research and development and science and technology-related activities. Public discussion may help in the development of such measures and might encourage public acceptance of them. Policymakers and administrators need to be cognizant of concerns about unintended consequences as they implement these initiatives. This report has explored such areas, including actions and proposals relating to foreign students; research laboratories; access to student records; research with biological "select agents;" controlling access to information via restricted websites; classification of scientific and technical information; application of the Freedom of Information act; and export control. Several kinds of scientific and technical professional association activities that could contribute to enhancing scientific and technical capability to deal with terrorism were identified.

---

[203](...continued)
and Synthetic Organic Chemical Manufacturers Association. For additional information see [www.chemistry.org/vulnerability.html].

[204][http://www.asce.org/publicpolicy/fedletters.cfm].

[205] Siri Carpenter, "Behavioral Science Gears Up to Combat Terrorism," *APA Monitor*, Nov. 10, 2001.

[206][http://www.apa.org/psychnet/coverage.html].