



OCTOBER  
1999

## GMOs Under a Microscope

The recent wave in Europe, Australia, and Japan against food items that contain genetically modified organisms (GMOs) — organisms within plant or animal systems that have had its DNA altered through gene splicing — has rippled into the United States. *Consumer Reports* published an article in September on the benefits and risks to public health from GMOs, and the scientific journal *Nature* reported that genetically modified corn might harm monarch butterflies in addition to unwanted insects. In response to heightened interest and media coverage, the Senate Committee on Agriculture conducted hearings on the regulatory system that both monitors the research as well as its incorporation from the field into food products and ultimately onto consumer shelves.

Since the Austrian monk Gregor Mendel conducted his experiments on pea plants, genetic research involving plant and animal systems has been an important field of science for improving agriculture and livestock. Conventional techniques such as selective breeding have been utilized for

hundreds of years to create heartier plants and healthier animals to improve both yield as well as resistance to disease and pests. These crossbreeding techniques, however, involve the transfer of genetic material in its entirety, both wanted and unwanted. With the advent of biotechnology tools such as gene splicing, modern techniques now allow scientists to transfer selected genes from one organism to another for a specific desired trait.

An example of this new technique, as well as one of the most controversial, involves transgenic corn. In this case a variety of corn was genetically modified to produce the natural protein *Bacillus thuringiensis (Bt)*, found in soil bacterium, to create an insect-resistant crop that would not require the use of chemical sprays. Another use involves altering a plant to be resistant to the herbicide *Roundup®*, allowing farmers to spray for weed control without harming crops. Researchers also have been able to beef up rice with certain vitamins that are absent from diets of less developed coun-

[GMOs, continued page 2](#)

## White House Revamps Encryption Policy

On September 16, 1999, the Clinton Administration radically revamped the current export control policy on encryption products. Perhaps as a nod to strong congressional support for H.R. 850, the Security and Freedom through Encryption (SAFE) Act, the White House proposal conforms somewhat to the SAFE Act's goals. The administration's proposed changes include easing export restrictions for retail products, allowing a higher bit standard for encryption exports, and supporting decryption technologies for law enforcement agencies.

In order to accomplish its goals, the White House plans to take a two-pronged approach. The first is to draft a new export control regulation by December 15<sup>th</sup> for public comment. The second is to have the administration's proposed legislation that sets standards for government access to decryption keys, the Cyberspace Electronic Security Act (CESA), passed through Congress.

The proposal would decontrol any encryption under 64 bits long, thereby raising the existing

standard from 56 bits and bringing it into compliance with the Wassenaar Agreement, a multinational treaty on export controls. In addition, 64-bit encryption products could now be imported under a license exception after a one-time technical review, a proposal that was also included in the SAFE Act. The only exception to this rule is that encryp-

[ENCRYPTION, continued page 3](#)

### Also In This Issue Page

<a href="#">Computer Security</a> .....	4
<a href="#">Commerce to Close NTIS</a> .....	5
<a href="#">Status of Major Legislation</a> .....	6
<a href="#">Reports and Publications</a> .....	7
<a href="#">Heard Off the Hill</a> .....	8



tries, allowing for the potential to improve global nutrition.

Under the 1986 "Coordinated Framework for Regulation of Biotechnology" new biotechnology products are regulated under existing procedures established through federal statutes and regulations. Hence, three federal agencies are responsible for the regulation of plants and foods created through agricultural biotechnology: the United States Department of Agriculture (USDA), the Food and Drug Administration (FDA), and the Environmental Protection Agency (EPA). Each agency acts independently and is responsible for a specific aspect of the process, although they are to coordinate activities. USDA regulates the field testing of genetically engineered plants and certain organisms, and ensures the safety of meat and poultry consumed as food. FDA, on the other hand, is responsible for the safety and labeling of drugs, as well as the safety of food and feed supply (excluding meat and poultry). EPA ensures that insecticides and herbicides are safe for humans to use with minimal adverse impact to the environment as a whole.

The FDA's legal authority to regulate genetically engineered food is governed by the Federal Food, Drug and Cosmetics Act. Under the act, the agency monitors food safety under two conditions, adulteration and food additives. Dr. James Maryanski, Biotechnology Coordinator for FDA'S Center for Food Safety and Applied Nutrition, testified that they require premarket approval of food additives that have "unusual chemical functions, have unknown toxicity, or would be new major dietary components of the food." By FDA standards, GMOs incorporated into foods to date have been altered with "well-characterized" proteins, fats, and carbohydrates that function similar to others already consumed. Hence, the FDA regulates bioengineered foods in the same manner as their conventional counterparts.

The EPA regulates biotechnology products through three sets of rules; two of which are finalized and a third expected to be finalized early next year. It regulates field testing of microbial pesticides under the Federal Insecticide, and Fungicide Act (FIFRA), and microbial biotechnology products through the Toxic Substances and Control Act (TSCA). Under FIFRA, EPA examines ecological effects for exposure and toxicity of plant-pesticide products and its impact to wildlife and "beneficial" insects. For example, the impact of *Bt* protein to monarch butterflies would fall under this category.

The potential adverse impact to monarch butterflies was first reported through a laboratory

study conducted by researchers at Cornell University. Dr. Janet Andersen, EPA's Director of the Biopesticides and Pollution Prevention Division, testified that the EPA "was aware of potential adverse effects on some species of butterflies, [but] did not believe that *Bt*-crops would threaten the long-term survival of the population of these species." In response to the Cornell study, EPA is using the opportunity to conduct exposure assessments in the field and are requesting data from registrants of *Bt* corn. Dr. Andersen stated that researchers acknowledged "that it would be inappropriate to draw conclusions about risk to monarch populations in the field solely on the initial results of their laboratory findings."

Proponents of agricultural biotechnology envision a future that allows farmers to utilize fewer chemicals thereby improving the environment, and to enhance the nutritional value of many plants that are consumed worldwide. Opponents see the unknown and the unanswered, especially between what is considered safe and unsafe. Mark Silbergeld of the Consumers Union of the United States, publisher of *Consumer Reports*, acknowledged before the Senate Agriculture Committee that this burgeoning field does hold opportunities. These opportunities, however, come with risk and Silbergeld expressed concern that "commercial product development and marketing...are well ahead of

GMOs, continued page 5

*Science & Technology in Congress* (ISSN# 1096-0406) is published by the Center for Science, Technology, and Congress at the American Association for the Advancement of Science (AAAS). It is distributed eight times per year: February through August and October. Issue Updates are published periodically to supplement the bulletin.

AAAS is a non-profit, non-partisan organization. Since it was founded in 1848, AAAS has been dedicated to the advancement of scientific knowledge for the good of society as a whole. Comments and suggestions on the bulletin and information on upcoming congressional science and technology activities are welcome. This bulletin has not been reviewed or endorsed by the AAAS Board or Council.

To subscribe, contact the Center for Science, Technology, and Congress at 202/326-6600. Subscriptions are free for congressional staff; \$40 for others. Please send address changes to: *Science & Technology in Congress*, AAAS, 1200 New York Avenue, NW, Washington, DC 20005; telephone: (202) 326-6600; fax: (202) 289-4950. Internet: [congress\\_center@aaas.org](mailto:congress_center@aaas.org). Information about the Center is also available on Internet at [www.aaas.org/spp/dspp/cstc/cstc.htm](http://www.aaas.org/spp/dspp/cstc/cstc.htm).

Albert H. Teich, Director  
Science and Policy Programs

Joanne Padrón Carney, Assistant Director

Leandro Lagera, Project Assistant

David G. Cooper, Intern



tion products cannot be exported to the "Terrorist 7" nations that support terrorism. Finally, foreign nationals no longer need an export license to work for U.S. firms on encryption.

CESA, on the other hand, addresses the problems faced by law enforcement and national security offices with the easing of export restrictions. The act would create a mechanism whereby third key access is possible along with an assurance of privacy for the key holder. CESA attempts to make it more difficult for government access to encryption keys being held by third parties entrusted with them for safekeeping, by requiring a court order first. Currently, keys held by third parties can be accessed with something as simple as a grand jury subpoena, whereas CESA would create a greater burden akin to requesting a wiretap or a search.

CESA also protects techniques used by law enforcement for decoding encryption. In some circumstances a key may not be stored with a third party, however, law enforcement authorities argue they still need to be able to gain access to encrypted material. Officials posit that techniques used to gain access must be kept confidential in order to prevent criminal elements from creating a counteragent. CESA ensures that these techniques be made secret, and requests funds to ensure that U.S. authorities keep pace with the rapid development of encrypting and decoding technologies.

Reaction to the administration's new policy seems to be cautious at best. Supporters for the SAFE Act and a looser encryption policy see this as a good sign and a significant step towards achieving their goals, but they are also waiting to see if truly substantive changes are implemented. "This announcement is long on potential but short on detail, and Congress will be watching carefully to make sure that the regulations issued in December match the policy announced today," warned Rep. Bob Goodlatte (R-VA), one of the primary sponsors of the SAFE Act, in a press release. In fact, some would like to proceed with passage of the act and not wait for the administration's guidelines. In a letter to the Speaker of the House, Rep. Randy "Duke" Cunningham (R-CA) lobbied to bring the SAFE Act to the floor for a vote simply because "[p]eople do not entirely trust the Clinton-Gore Administration to establish regulations that live up to its policy promises."

Thomas J. Donahue, President of the U.S. Chamber of Commerce, in a letter to Rep. Goodlatte, pointed out that the SAFE Act addresses several issues that the new policy does not. Topics such as

codifying the policy, providing a time-frame for technical review, preventing the government from mandating the use of certain types of encryption, and prohibiting mandatory key escrow accounts are lacking. "We are concerned that loosening export controls on encryption products through the regulatory process without the legislative safeguards contained in H.R. 850 could be detrimental to the long-term interest of the business community," argued Donahue.

The administration counters that the new policy properly balances the interests of all parties involved. It tries to meet privacy and security concerns of the public, while allowing law enforcement officials the chance to do their job. Attorney General Janet Reno called the new policy, "a balanced approach which will encourage the use of encryption but protect national security and public safety." One of the SAFE Act's most ardent supporters, Americans for Computer Privacy, seem to concur with the Attorney General. "This development is the new policy America needs to maintain its technological leadership, strengthen the government's abilities to protect our critical infrastructure, and fight crime in the Information Age," said the group in a released statement.

However, there are those that are wondering if the administration is not caving in to the demands of high-tech industry and sacrificing national security needs. Rep. Curt Weldon (R-PA) strongly voiced his concern that the United States is giving up its edge in information security. "I'm not convinced that what we're doing here is necessary and logical," griped Rep. Weldon, "I want to be absolutely certain that we maintain our information superiority." Rep. Weldon demanded that representatives from the Central Intelligence Agency and the National Security Agency, two agencies adamantly opposed in the past to changing encryption policy, be made to appear at a public hearing so that he may question them on their position.

For now, most interested parties are taking a wait and see approach. William Reinsch, Undersecretary for the Department of Commerce, said that they expect to complete the draft regulation by December 15, 1999, as originally announced and allow opportunity for public comment. As it stands now, it looks as if the administration has done an about face due to immense political pressure from supporters of H.R. 850, which has amassed 258 co-sponsors, but until a final and concrete regulation is written, the administration's rhetoric could simply be just that. ■



# House Bill Would Strengthen Computer Security

Since passage of the Computer Security Act (1987), the National Institute of Standards and Technology (NIST) has been responsible for setting computer security standards for the protection of sensitive but unclassified information at federal agencies. To enable NIST to better address today's security needs, Rep. F. James Sensenbrenner, Jr. (R-WI), Chairman of the House Committee on Science, has introduced the Computer Security Enhancement Act of 1999.

The bill, co-sponsored by Representatives Bart Gordon (D-TN) and Constance A. Morella (R-MD), Chairwoman of the Science Committee's Subcommittee on Technology, would amend the National Institute of Standards and Technology Act to emphasize the importance of information security and the development in industry of encryption technology. It aims to make computer security technology more available and less expensive for federal agencies by requiring NIST to promote the use of commercial off-the-shelf products. The underlying principle of the act, according to Rep. Gordon, is that public and private sector security needs are very similar, and that cooperation between government and industry can lead to better security for both.

It further requires NIST to develop guidelines for federal agencies to follow when using any electronic authentication technology and establishes a National Policy Panel for Digital Signatures. In addition, it would commission a study by the National Research Council (NRC) of public key infrastructure. The NRC study would assess technology to support key infrastructure, current deployment plans, and federal action needed to ensure its feasibility, as well as any other topics NRC considers relevant.

The issue of computer security was brought sharply into focus after several incidents last spring and summer. The "Melissa" computer virus affected the e-mail and files of thousands of computer users, including some at federal agencies. The web sites of the White House, Senate, and several agencies were altered by hackers who left anti-government messages. While these attacks caused no major damage, they demonstrated the vulnerability of the federal government's computer systems.

At a hearing held on September 30 by the Subcommittee on Technology, NIST Director Raymond Kammer, Keith Rhodes, director of the General Accounting Office's Office of Computer and Information Technology Assessment, Harris Miller, president of the Information Technology Association of

America, and Prof. George Trubow, of the John Marshall Law School in Chicago, all testified in support of the general thrust of the act, but raised several significant reservations.

Mr. Kammer identified several potential problems regarding NIST's redefined role. The bill requires NIST to coordinate the federal response to security problems in federal computer systems. Mr. Kammer stated that NIST could "play an important role in developing guidance" on these response efforts, but that it would be inappropriate to put NIST in a "central operational capacity" in developing responses to specific problems. "Agencies need to have programs and procedures in place, drawing upon NIST guidance, to address such situations," he said. In addition, the bill limits the authority of NIST by prohibiting it from adopting encryption standards required for use in computer systems outside the federal government. While Mr. Kammer supports the intent of this clause, he expressed concern that the language could be interpreted to preclude collaboration with the private sector.

The measure also gives the Computer System Security and Privacy Advisory Board a greater role in advising NIST. The original version of the act would have required NIST to solicit written recommendations from the Board before finalizing any guidelines or standards, a clause Mr. Kammer said might delay the adoption of important, non-controversial standards. It was struck from the bill at an October 20 mark-up session. Finally, Mr. Kammer expressed concern that establishing the digital signatures panel could be interpreted as authorizing the writing of standards for the private sector.

Mr. Miller and Prof. Trubow, who is a member of the Advisory Board, also expressed some reservations about the bill. Mr. Miller suggested that the bill direct NIST to develop "guidelines" for encryption technology rather than "standards" because he is concerned that the term "standards" would tend to freeze the growth of new technology in the private-sector. Prof. Trubow suggested that the act include strengthening privacy, as well as security, as one of its stated goals.

The version of the Computer Security Enhancement Act currently under consideration, H.R. 2413, combines an earlier version passed by the House in 1997 that never reached the floor of the Senate with the Digital Signature Act of 1999 (H.R. 1572), introduced by the Science Committee earlier this year. The act passed the Technology Subcommittee and has been sent to the full Science Committee. ■

# Commerce Proposes to Close NTIS



The Department of Commerce announced in August that it plans to close its National Technical Information Service (NTIS) at the end of fiscal year (FY) 2000. Created in the 1950's, NTIS is the central clearinghouse of U.S. and international scientific and technical information. Unfortunately, the role of NTIS as archivist and disseminator of information was weakened by two important events. First, a 1987 congressional mandate requiring NTIS to support its operations by revenues received through publication sales rather than federal appropriations. Second, the dawn of the Internet and the ability to access and acquire information of all kind directly through federal agency web sites at no cost.

The NTIS centralized collection currently consists of over 3 million documents ranging from federally funded scientific reports, statistical data, federal standards, and international research abstracts. Since the 1987 congressional mandate, however, NTIS has expanded its collection to include documents that are not necessarily science and technology specific in order to generate revenue. Today, two of its largest sources of revenue are from projects coordinated with *FedWorld* and the Internal Revenue Service. Between 1993 and 1998, NTIS revenues dropped 18 percent while sales of publications dropped by 43 percent. With the increased presence of the federal government on the Internet, many research and development agencies are bypassing NTIS and placing reports and publications

directly on their own web sites. As a result, the number of reports received by NTIS from other agencies has declined 34 percent in the same time frame.

Many of these reports are free from the sponsoring agency, whereas the taxpayer would have to pay if obtained through NTIS. For example, *The Emerging Digital Economy*, is free from Commerce, but costs \$27.00 through NTIS. Robert Mallett, Deputy Secretary of Commerce, summed up the situation in a very candid manner before an October 21 hearing of the Senate Commerce Subcommittee on Science, Technology and Space. "If it were my money, I know what I would do. This, in a nutshell, sums up the problem facing the NTIS."

Commerce has prepared draft legislation that outlines its proposed three-pronged strategy for closing down the clearinghouse. First, transfer the entire collection to the Library of Congress, including all paper, microfiche, and digital documents, as well as the NTIS bibliographic database. Second, make certain that current and future information is electronically stored at the Library. And finally, work with existing federal agencies to ensure that its scientific, technical, and business information is posted on the Internet for a minimum of three years. The library community has expressed concern about the proposed closure and question whether the new location for the collection will actually solve the problem of costs. ■

---

## GMOs, from page 2

the policies needed to assure public health, environmental safety and the rights of consumers."

One public health concern is allergenicity. Incorporating GMOs into other plant systems, if not regulated properly, could raise the potential risk that proteins with allergens be transferred. Another public health concern is toxicity. Plants that contain natural toxic substances at extremely minute levels may see those levels increase over time after genetic alteration. The FDA is aware of these concerns and recommends that developers consult with the agency in the early development phase. Environmental concerns surround the creation of new super weeds and insects that could develop resistance after long-term exposure in the same way that some bacteria develop resistance to antibiotics over time. EPA is conducting experiments involving the planting of mixed crops to mitigate resistance.

Fear of consumer backlash prompted some foreign and U.S. companies to cease incorporating GMOs into their food products. The Monsanto Com-

pany, a leader in agricultural biotechnology, recently stated that it would no longer conduct research into controversial "terminator" seeds that sterilize after one generation. Some European nations have established trade barriers to inhibit the importation of GMOs, and others have taken the position that food products that contain GMOs in amounts as little as 1 percent are required to have labels.

Consumer groups in the United States are joining the bandwagon and requesting that our nation set a labeling standard. They believe that the upcoming World Trade Organization talks in Seattle, WA at the end of November is a ripe opportunity to address this issue at the global level.

How much should the consumer know, however, is a hotly debated topic. The FDA announced in the Federal Register plans to conduct a series of public meetings over the next two months to discuss whether its policies and procedures should be modified, as well as mechanisms for informing the public (e.g., labeling). A meeting in Washington, DC is scheduled for November 30. ■



# Status of Major Legislation

## CYBER SECURITY

### SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT

#### H.R. 850

Introduced by Rep. Bob Goodlatte (R-VA). A bill to amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption. 2/25/99 Referred to the Committees on the Judiciary, and International Relations. 3/24/99 Ordered to be reported by Judiciary Committee. 4/27/99 Referred jointly and sequentially to the House Committee on Intelligence (Permanent Select), the House Committee on Commerce, and the House Committee on Armed Services. 6/23/99 Ordered to be reported (Amended) by the Commerce Committee. 7/13/99 Ordered to be reported (Amended) by International Relations Committee.

### COMPUTER SECURITY ENHANCEMENT ACT OF 1999

#### H.R. 2413

A bill to amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes. 7/1/99 Referred to the Committee on Science. 9/30/99 Hearings Held by the Subcommittee on Technology Prior to Referral. 10/20/99 Forwarded by Subcommittee to Full Committee (Amended) by Voice Vote.

### TRADEMARK CYBERPIRACY PREVENTION ACT

#### H.R. 3028

Introduced by Rep. James E. Rogan (R-CA). A bill to amend certain trademark laws to prevent the misappropriation of trademarks. 10/6/99 Referred to the House Committee on the Judiciary. 10/13/99 Ordered to be Reported (Amended) by Voice Vote.

## INFORMATION TECHNOLOGY

### NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT ACT

#### H.R. 2086

Introduced by Rep. F. James Sensenbrenner, Jr. (R-WI). A bill to authorize funding for networking and information technology research and development for fiscal years 2000 through 2004. 6/9/99 Read twice and referred to the Committees on Science, and Ways and Means. 9/9/99 Ordered to be Reported (Amended) out of the Science Committee by the Yeas and Nays: 41 - 1.

## BASIC RESEARCH

### FEDERAL RESEARCH INVESTMENT ACT

#### S. 296

Introduced by Sen. Bill Frist (R-TN). A bill to provide for continuation of the federal research investment in a fiscally sustainable way, and for other purposes. 7/26/99 Passed Senate with amendments by unanimous consent. 7/27/99 Referred to the House Committee on Science.

## DEFENSE

### FY2000 DEFENSE AUTHORIZATION BILL

#### S. 1059

Introduced by Sen. John W. Warner (R-VA). An original bill to authorize appropriations for fiscal year 2000 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe personnel strengths for such fiscal year for the Armed Forces, and for other purposes. 10/05/99 Public Law 106-65.

## E - C O M M E R C E

### COLLECTIONS OF INFORMATION ANTIPIRACY ACT

#### H.R. 354

Introduced by Rep. Howard Coble (R-NC). A bill to amend title 17, United States Code, to provide protection for certain collections of information. 10/08/99 Committee on Commerce discharged in House.

### CONSUMER AND INVESTOR ACCESS TO INFORMATION ACT OF 1999

#### H.R. 1858

Introduced by Rep. Tom Bliley (R-VA). A bill to promote electronic commerce through improved access for consumers to electronic databases, including securities market information databases. 10/08/99 Committee on the Judiciary discharged in House.

### ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT

#### H.R. 1714

Introduced by Rep. Tom Bliley (R-VA). A bill to facilitate the use of electronic records and signatures in interstate or foreign commerce. 10/15/99 Reported (Amended) by the Committee on Judiciary, H. Rept. 106-341, Part II. Placed on the Union Calendar, Calendar No. 222. 11/1/99 On motion to suspend the rules and pass the bill, as amended, failed by Yeas and Nays. ■

# Reports and Publications

## CONGRESSIONAL RESEARCH SERVICE

Copies of CRS reports for congressional use are available by calling 202/707-7132.

*Patent Ownership and Federal Research and Development (R&D): A Discussion on the Bayh-Dole Act and the Stevenson-Wydler Act (RL30320).* This report provides an overview of these two laws in order to facilitate a better understanding of the framework within which decisions are made concerning patent ownership and licensing.

*Satellite-Delivered Television: Issues Concerning Consumer Access to Broadcast Network Television via Satellite (98-942 STM).* This report summarizes issues surrounding attempts to revise the 1988 Satellite Home Viewer Act (SHVA), which prevents certain households from receiving broadcast network signals via satellite.

*Y2K Challenges and Transportation: Risks and Solutions (RS20184).* This report examines the extent of Y2K problems in transportation systems. Estimates suggest that at least \$1 billion of private sector, transit authority, and federal funds have been or will soon be allocated to assess and fix these problems.

## GENERAL ACCOUNTING OFFICE

Copies of GAO Publications are available by calling 202/512-6000 or via the Internet at <http://www.gao.gov>.

*Defense Acquisitions: Comanche Program Cost, Schedule, and Performance Status (NSIAD-99-146).* This report reviews the status of the Comanche helicopter program. It assesses the Army's restructured plans for developing and testing, changes in performance capabilities and requirements, cost estimates for development, and impact on aviation modernization efforts. It finds that the program contains significant risks of cost overruns, schedule delays, and degraded performance.

*Foreign Military Sales: Review Process for Controlled Missile Technology Needs Improvement (NSIAD-99-231).* This report looks at how the Foreign Military Sales program safeguards technology and arms transfers. Over the years, the U.S. government has sold certain sensitive military items through this program presuming better control than if sold commercially. However, the process for making decisions about what technology may be transferred under the program is not readily understood.

*Nuclear Nonproliferation: Status of Transparency Measures for U.S. Purchase of Russian Highly Enriched Uranium (RCED-99-194).* This report examines existing and proposed transparency measures to verify the completion of Russia's agreement to sell

about \$12 billion of highly enriched uranium to the U.S. Highly enriched uranium is diluted to low enriched uranium before shipment, and it is necessary for the U.S. to verify it before receipt. The report finds, however, that several key monitoring measures have not yet been put into place.

*Environmental Protection: Assessing Impacts of EPA's Regulations Through Retrospective Studies (RCED-99-250).* This report looks at the desirability of conducting retrospective cost-benefit analyses of EPA regulations. The report finds that such retrospective studies can be useful but that obtaining valid cost data and quantifying actual benefits can be difficult. It recommends that EPA develop a systematic approach to foster retrospective studies in the future.

## NATIONAL ACADEMY OF SCIENCES, NATIONAL ACADEMY OF ENGINEERING, INSTITUTE OF MEDICINE, NATIONAL RESEARCH COUNCIL

Government offices may obtain single complimentary copies by calling the Office of Congressional and Government Affairs at 202/334-1513. Others may order copies from the National Academy Press by calling 800/624-6242 or via the Internet at <http://www.nap.edu>.

*The Pervasive Role of Science, Technology, and Health in Foreign Policy: Imperatives for the Department of State (ISBN 0-309-06785-5).* Concerns about nuclear nonproliferation, industrial competitiveness, climate change, energy, infectious diseases, and space exploration require increased technical competence within the State Department. This report suggests ways to make science, technology, and health considerations an integral part of the nation's foreign policy.

*Perspectives on Biodiversity: Valuing Its Role in an Everchanging World (ISBN 0-309-06581-X).* This report reviews current understanding of the value of biodiversity and the methods that are useful in assessing that value in particular circumstances. Many federal and state agencies have lands held in large blocks where biodiversity can be protected and maintained. Their importance aesthetically, economically, and biologically should not be undervalued.

*Science for Decisionmaking: Coastal and Marine Geology at the U.S. Geological Survey (ISBN 0-309-06584-4).* This report attempts to provide an understanding of the importance of the geologic sciences in understanding the coastal and marine areas of the United States. These areas are some of the most resource-rich in the nation, and the ability to manage them wisely will lie in a scientific understanding of the processes that control the distribution and functioning of their enormous wealth.



## HEARD OFF THE HILL



---

An important step has been made towards understanding how damaged DNA is identified and removed by healthy cells. Researchers at the University of Texas Southwestern Medical Center have determined the molecular structure of a critical enzyme in the genetic repair process. Enzyme UvrB travels along strands of DNA and binds tightly to damaged areas, alerting other molecules to slice the segment out of the genetic code. DNA is corrected constantly to protect organisms from cancer-causing mutations, and understanding the molecular basis of this process could lead to better cancer therapies in the future. *EurekAlert* October 12, 1999.

Engineering students at North Carolina State University have designed a robot that creeps through gas and water pipes while listening for sounds of human life. Inspired by media accounts of rescuers unable to locate living victims in the 1995 Oklahoma City federal building bombing, the robot's purpose is to help find trapped survivors in buildings damaged by bombs or earthquakes. The robot, named MoccasinII, contains a microphone and video camera that can be monitored from a remote location. *New Scientist* October 2, 1999.

---

University of California at Berkeley researchers have created video images of the world through the eyes of a cat. While the cat was positioned to look at an experimenter's face and other objects, electrical activity in a visual processing region of its brain was recorded. The recording electrodes were attached to a computer which used a "linear decoding technique" to produce fuzzy but recognizable images of what the cat was seeing. The potential applications of this experiment include everything from using rats to check on subway repairs to wiring machines directly to people's brains to be controlled by their thoughts. *BBC* October 11, 1999.

A deliberate crash of the Lunar Prospector spacecraft into a moon crater failed to prove the presence of water on the moon. Water is a critical need of future refueling stations and colonies, and University of Texas astronomers had hoped to observe a spray of water-laden dust which would confirm other indications of underground water in the crater. In a separate experiment, high-resolution pictures taken by NASA of Mars showed that landmarks earlier believed to be ancient coastlines were not caused by water after all. *CNN* October 13, 1999. ■



AMERICAN ASSOCIATION FOR THE  
ADVANCEMENT OF SCIENCE

Center for Science, Technology, and Congress  
1200 New York Avenue, NW  
Washington, DC 20005

Address Change Requested

