

August 7, 2000

Dear *STC* Reader:

The Center for Science, Technology, and Congress is pleased to launch a new look for the *Science and Technology in Congress (STC)* newsletter. The revamped newsletter will provide some new services including:

- Scientific Definitions
- Updates on AAAS Reports & Events
- Website Links in Articles for Further Resource Information

In addition, the online version of the newsletter will contain hyperlinks that will direct you instantly to helpful resources, allowing our readers the ability to quickly locate important science and technology information. Also new to the online version is an e-mail service that alerts readers as soon as new content is posted. Though *STC* will no longer publish a "Status of Major Legislation" section in the printed version of the newsletter, readers will be able to track science and technology bills on the *STC* website.

The *Science and Technology in Congress* website address is:

www.aaas.org/spp/cstc/stc

STC will continue to provide coverage of science and technology policy issues within the executive and legislative branches, as well as a list of noteworthy reports and publications. The Center will also continue to publish eight issues a year, with occasional special issue updates.

We hope you enjoy the new look and services of *Science and Technology in Congress*. We welcome any comments, questions, or suggestions. You may contact us at 202/326-6600 or congress_center@aaas.org.

Sincerely,

Joanne Padrón Carney
Director
Center for Science, Technology, and Congress

David G. Cooper
Project Coordinator
Center for Science, Technology, and Congress

Science + Technology

IN CONGRESS

August
2000

Privacy Bills Move Forward

The House Banking and Financial Services Committee passed the Medical Financial Privacy Protection Act (H.R. 4585) on June 29, bringing protection of personal identifiable information a step closer to passage. H.R. 4585 would require insurance companies and financial institutions to obtain an individual's consent before sharing their medical records with third parties or affiliated companies. On the same day the House Government Reform Committee passed legislation (H.R. 4049) to create a commission to study a multitude of privacy issues, including medical privacy. Detractors of H.R. 4049 have expressed concern that the creation of a privacy commission would stall any real legislation from moving forward.

The Medical Financial Privacy Protection Act would amend Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801) by making it more difficult for insurance and banking institutions to disclose personal identifiable health information. The original Gramm-Leach-Bliley bill—which overhauled the financial services industry—required that consumers be allowed to opt-out before any personal information is shared with unaffiliated organizations. As a result of the financial modernization law, health and life insurers can now merge with banks and other financial service institu-

tions. Concern grew that these new conglomerates could utilize personal medical information to determine whether to issue life insurance, loans, or a mortgage.

H.R. 4585 as passed by the committee would expand the original opt-out provision to include data shared with affiliated companies. In addition, the committee adopted an amendment that would permit individuals to sue their financial institutions for disclosing personal information without prior consent. Exemptions are included

in the legislation to allow these institutions to share medical records with state guaranty funds or to process worker compensation claims and some aspects of group health plans. H.R. 4585 also provides customers of these institutions the right to access and correct their personal identifiable information.

The Medical Financial Privacy Protection Act differs from other medical privacy bills in that it relates strictly to medical infor-

>>> *Continued on page 4*

Cyber Security Bill To Amend FOIA

As part of an ongoing movement to improve security of the nation's computer infrastructure, a new bill has been proposed in the House to encourage private sector participation in information sharing centers. The legislation, introduced by Reps. Tom Davis (R-VA) and Jim Moran (D-VA), would exempt certain information about cyber security from disclosure under the Freedom of Information Act (FOIA), allowing private firms to share information with the federal government that they do not wish to make public. While the bill has received support from the business and high tech communities, some privacy advocates have argued that it is unnecessary and might weaken FOIA.

Entitled the Cyber Security Information Act of 2000, the bill (H.R. 4246) is modeled after the Y2K Information Readiness and Disclosure Act (Public Law 105-271), which was designed to promote partnerships between government and industry to address the Y2K problem. The Y2K bill established antitrust, liability, and FOIA exemptions for Y2K-related information, in an attempt to facilitate information sharing among companies fearful that information released to the public could be used against them in lawsuits. Like the

>>> *Continued on page 6*

FEATURES

- | | | | |
|---------|------------------------|---|----------------------------|
| 1, 4 | Privacy Bills | 3 | Gordon Takes Reins at NNSA |
| 1, 6, 7 | Cyber Security Bill | 5 | Reports + Publications |
| 2, 4 | Genetic Discrimination | 6 | Scientific Definitions |
| 2 | E-Signatures | 8 | Heard Off the Hill |

"This is a great job. ... I get to work with superb people. I have no small degree of influence over the best science laboratories in the country."

TURN TO PAGE 3 FOR THE FULL STORY

Genome Progress Raises Ethical Concerns

On June 26, the Human Genome Project announced that approximately 85 percent of the entire human genome had been sequenced, laying out a draft road map for future research into potential therapeutic applications. Barely a month later, the Senate Health, Education, Labor, and Pensions Committee held a hearing to discuss the project, the knowledge it carries, and its potential adverse impact—discrimination against potential and perceived disabilities by employers and insurance companies.

Dr. Francis Collins, Director of the National Human Genome Research Institute at the National Institutes of Health, heads

“Already, with but a handful of genetic tests in common use, people have lost their jobs, lost their health insurance, and lost their economic well being due to the unfair and inappropriate use of genetic information.”

the Human Genome Project that produced the sequencing breakthrough. Dr. Collins has long been outspoken about the need for legislative protection against genetic discrimination and his July 20 appearance before the Senate committee proved no less. He testified that while genetic research holds great promise, it can “also be used in ways that are fundamentally unjust. ... Already, with but a handful of genetic tests in common use, people have lost their jobs, lost their health insurance, and lost their economic well being due to the unfair and inappropriate use of genetic information.”

Both Collins and Senate Democratic Leader Tom Daschle (D-SD) provided a list of examples of individuals who had been discriminated against based on genetic disease traits that they carried. Sen. Daschle stated in his opening remarks before the

committee, “As the use of genetic tests increases, the number of genetic discrimination victims will increase unless we specify—clearly and unambiguously—how genetic information may be used—and how it may not be used.”

Not only is potential discrimination at issue, but also the future of genetic research if people opt out of participating in studies for fear of how the information will be used. This is a real concern to scientists working in this burgeoning field, as noted in Sen. Daschle’s testimony. Dr. Craig Venter, president of Celera Genomics, a private firm involved in sequencing the genome, wrote a letter to the senator stating, “This is not a theoretical concern. Today, people who know they may be at risk for a genetic disease are forgoing diagnostic tests for fear they will lose their job or their health insurance.”

To protect against the potential misuse of genetic information, Sen. Daschle, along with Senators Edward Kennedy (D-MA), Christopher Dodd (D-CT), and Tom Harkin (D-IA), has introduced the Genetic Nondiscrimination in Insurance and Employment Act (S. 1322). His bill would extend the same protections to the private sector given to government employees by executive order (E.O. 13145). S. 1322 would make it

illegal for an employer to discriminate against new applicants or fire existing employees based on genetic information, prohibit disclosure of an employee’s genetic information without prior consent, and allow employees the right to sue for discrimination in court. In addition, the bill would not allow insurance companies to deny coverage based on a person’s genetic trait.

On the House side, Rep. Louise Slaughter (D-NY) introduced the Genetic Nondiscrimination in Health Insurance and Employment Act of 1999 (H.R. 2457) last session. Rep. Slaughter is the original champion of the cause, although neither her bill nor Sen. Daschle’s has successfully moved through committee. Recently, Sen. Daschle attempted to introduce an amendment similar to S. 1322 to the Labor, Health and Human Services, Education appropriations bill, however, it failed on the Senate floor along party lines.

Though all witnesses at the hearing attested to the fact that discrimination based on an individual’s genetic makeup is wrong, the appropriate legislative vehicle to protect against such acts is a contested matter. It was noted that the Americans with Disabilities Act (ADA) may provide some limited coverage. For example, a genetic

>>> *Continued on page 4*

President Signs Electronic Signatures Bill

On June 30, before an audience at the Independence National Historical Park in Philadelphia, President Clinton signed into law S. 761, the “Electronic Signatures in Global and National Commerce Act.” The new law removes legal impediments by providing the same legal standing for digital signatures that exists for paper signatures. Hence, electronic contracts will carry the same legal weight as paper contracts.

S. 761 governs only commercial transactions and not government activities, and requires both federal and state governments to prescribe standards and other regulations necessary to prevent waste and fraud, enforce the law, and protect consumers.

Passage of the “Electronic Signatures in Global and National Commerce Act” heralded an almost unprecedented bipartisan and bicameral support and was eagerly awaited by an Administration that has trumpeted its enactment as a major step to fully develop electronic commerce. President Clinton stated at the signing ceremony, “This Act demonstrates that we can achieve the full measure of the benefits that electronic commerce has to offer, if we marry one of our oldest values—our commitment to consumer protection—with the newest technologies.” •••

Gordon Takes NNSA Reins, Tensions Ease on Hill

With the swearing in of Gen. John Gordon as Administrator of the National Nuclear Security Administration (NNSA), the long-running struggle between Secretary of Energy Bill Richardson and Congress over the nation's nuclear security appears to have abated for the time being. Gen. Gordon, who was confirmed by the Senate on June 14 after a long delay, started his new position on June 28, and delivered his first congressional testimony as NNSA Administrator just two weeks later, the day before his formal swearing-in on July 12.

NNSA is a new semi-autonomous agency within the Department of Energy (DOE) tasked with oversight of the nation's

Duncan Hunter's (R-CA) Nuclear Secrets Safety Act (H.R. 4737), which would require an inventory of sensitive documents and hardware at the national laboratories and tighten security around vaults containing sensitive information. Also approved by the committee was H.R. 3906, which would establish an independent oversight office at NNSA modeled after the DOE Office of Independent Security Oversight.

Perhaps the most contentious issue between Congress and the secretary has been "dual-hatting," the assignment of top officials to both NNSA and non-NNSA positions. The practice has been attacked from both sides of the aisle as contrary to the letter and intent of the reorganization, but vigorously defended by Sec. Richardson as a means of maintaining sound department-wide policy. On June 27, the House amended the FY 2001 Energy and Water Development appropriations bill to explicitly prohibit "dual-hatting," an action also taken by the Senate in the FY 2001 defense authorization bill.

Tension over the dual-hatting issue appeared to dissipate, however, with Gen. Gordon's July 11 testimony before the Special Oversight Panel on Department of Energy Reorganization of the House Armed Services Committee. The new administrator promised to eliminate dual-hatting by filling the top NNSA security positions with individuals working only within NNSA. "[D]ual-hatting is not going to be a problem," he assured the panel.

Gen. Gordon used the testimony to present a rough outline of his plans. His first action, he said, would be to visit Los Alamos and give notice that "there are changes afoot." Improving security means finding a way to "convince folks [at the labs] to take this upon themselves." He identified three major problem areas that the new agency must address: aging infrastructure, difficulty attracting the best personnel, and

a lack of full support in Congress. Gen. Gordon's testimony drew unanimous praise from the members of the panel, who recognized the difficulty in cleaning up a department that ranking member Rep. Ellen Tauscher (D-CA) described as being "entangled in bureaucratic kudzu."

Gen. Gordon, who once worked as a physicist at Sandia National Laboratories, serves as DOE Under Secretary for Nuclear Security as well as NNSA Administrator. He assumed his position at NNSA after serving as second-in-command at the Central Intelligence Agency. He has spent much of his career working on nuclear weapons and arms control issues, and received support from virtually all quarters when Sec. Richardson announced his selection on March 2. Sen. Pete V. Domenici (R-NM), one of the architects of the reorganization, described him as "a superb choice" whose "qualifications are truly unique."

His confirmation, however, did not proceed without a glitch. Although formally nominated on May 4, his confirmation was delayed until June 14 by Sen. Richard H. Bryan (D-NV) because of objections to the dual-hatting prohibition in the Senate's defense authorization bill. Only after the hard drives went missing at Los Alamos did Sen. Bryan drop his objections, allowing Gen. Gordon to be confirmed by a vote of 97-0.

The new under secretary is realistic about the difficulty of his position, but was optimistic at his swearing in ceremony. "There certainly is no shortage of problems and issues to attack," he said. "But I cannot accept the premise that there is little chance of success or that the mission is not important or not worth our best efforts. ... This is a great job. ... I will continue to play a significant role in national security. I get to work with superb people. I have no small degree of influence over the best science laboratories in the country." •••

Tension over the dual-hatting issue appeared to dissipate with Gen. Gordon's July 11 testimony.

nuclear weapons facilities. It was created by Congress last fall in a reorganization intended to address DOE's security problems. However, Sec. Richardson has been sparring with members of Congress over its implementation for much of the last nine months. Several bills and amendments dealing with nuclear security have recently been passed, sometimes over objections from Sec. Richardson. The latest is H.Res. 534, a resolution that calls for the NNSA Administrator to take "immediate action" to address nuclear security deficiencies. In the wake of the disappearance of two computer hard drives from a classified facility at Los Alamos National Laboratory, the measure passed the House by an overwhelming margin, 391-5.

On June 28, the House Armed Services Committee passed four other bills relating to DOE security issues, including Rep.

FOR THE LATEST ON SCIENCE-RELATED BILLS...

...visit the Science and Technology in Congress *Status of Major Legislation* section at www.aaas.org/spp/cstc/stc/status.htm

FOR UP-TO-DATE INFO ON FEDERAL R&D FUNDING...

...check out the AAAS *R&D Budget and Policy Program* at www.aaas.org/spp/R&D

FOR MORE INFORMATION:

National Nuclear Security Administration (NNSA): www.nnsa.doe.gov

Los Alamos National Laboratory: www.lanl.gov

House Armed Services Committee: www.house.gov/hasc

Privacy Bills Move Forward

Continued from page 1

mation in financial institutions, whereas the proposed Department of Health and Human Services (HHS) regulation issued in November 1999, applies to health plans, health care providers, and health care clearinghouses.

The passage of H.R. 4585 met with immediate opposition from organizations such as the American Bankers Association, the American Council of Life Insurance, the American Insurance Association, and the Securities Industry Association. These trade groups contend that complying with Title V of the Gramm-Leach-Bliley bill is complex enough without imposing additional

These trade groups contend that it would be best to see how implementation of the original bill fairs before attempting to broaden it further.

onerous requirements, and that it would be best to see how implementation of the original bill fairs before attempting to broaden it further.

The expansion of the opt-out provision to encompass affiliate companies was also met with resistance. Insurance institutions argue that most financial service companies establish separate subsidiaries for tax or organizational objectives and that regulating the sharing of information among these affiliates essentially boils down to regulating within the business itself, placing additional and unwarranted burdens.

Finally, the trade groups fear that in the future, individual customers will be able to demand to see their personal medical records regardless of whether the institution is even utilizing them, requiring another layer of management.

The bill now goes to the House Commerce Committee, which should prove a tough battle given the vociferous industry opposition.

On the same day the medical financial privacy bill passed, the House Government Reform Committee voted to establish a Commission for the Comprehensive Study of Privacy Protection (H.R. 4049). The legislation would establish a 17-member commission appointed by the White House and Congress to conduct an 18-month study of issues "relating to protection of individual privacy and the appropriate balance to be achieved between protecting individual privacy and allowing appropriate uses of information." The commission is to focus on medical, educational, library, and purchase and payment records, as well as the use of other identifiers such as driver's license and credit cards. The study will address "the monitoring, collection, and distribution of personal information by Fed-

eral and State governments, individuals, or [other] entities," such as the private sector. The final report to be submitted to the President and the Congress is to include findings and recommendations regarding the potential threats posed to individuals, the effectiveness of existing statutes and regulations, and whether additional legislation is necessary. •••

FOR MORE INFORMATION:

House Banking and Financial Services Committee: www.house.gov/banking

White House Virtual Library: www.whitehouse.gov/library/index.html

HHS Medical Privacy Regulation: Federal Register, www.access.gpo.gov, Vol. 64, No. 212, 11/3/99, pp. 59917-60065

Genome Progress...

Continued from page 2

test or screening is considered a medical examination and the ADA contains provisions that control the way that an employer is allowed to conduct such examinations (e.g., in hiring practices).

A thornier issue, however, is that of the definition of disability. Discrimination against a person with a disability is clearly protected by the ADA. Though a genetic test may reveal whether one is predisposed to developing a disease or is a carrier of a hereditary disease, a positive test does not guarantee that the individual will develop the associated disease in the future. Hence, does it constitute discrimination under the ADA if an employer makes a hiring or firing decision based on the *potentiality* of a disability? The Equal Employment Opportunity Commission argued in its March 1995 Interpretative Guidance that an employer could be held liable merely by acting upon the perception of impairment. The limit of the ADA's scope, however, is debatable since this area of discrimination law is so new and has yet to be argued in court.

Harold P. Coxson, Esq., representing the law firm of Ogletree, Deakins, Nash, Smoak and Stewart, P.C., argued before the Senate committee that the capacity and limitations of the ADA to protect against genetic discrimination needs to be analyzed more thoroughly before additional legislation is approved. In addition, Coxson recommended either amending ADA to address gaps in the current law or pursuing medical record privacy legislation as a solution in lieu of a separate bill. "Other alternatives, such as medical record privacy legislation, should be considered as well, since the origin of any problem related to employment decisions based on genetic information is the dissemination of such confidential information in the first place," Coxson stated. •••

FOR MORE INFORMATION:

Senate Committee on Health, Education, Labor and Pensions: www.senate.gov/labor

National Human Genome Research Institute: www.nhgri.nih.gov

U.S. Equal Employment Opportunity Commission: www.eeoc.gov

CONGRESSIONAL RESEARCH SERVICE

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

- **Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth (98-67 STM)**
This report summarizes several key technology policy issues before the 106th Congress that could affect the growth and use of the Internet: encryption and electronic signatures, computer security, Internet privacy, protecting children from unsuitable material on the World Wide Web, unsolicited electronic mail, Internet domain names, and access to broadband services. It also includes a summary of related legislation.
- **Internet Privacy—Protecting Personal Information: Overview and Pending Legislation (RS20035)**
Growing use of computers and the Internet is raising concerns about the privacy of personal information collected when using the Internet or stored on computers. This issue brief discusses the various topics surrounding Internet privacy and legislation introduced to protect it.
- **The National Aeronautics and Space Administration (NASA): History and Organization (RL30577)**
This report provides an overview of the agency including a brief history of its activities since inception, a breakdown of its major programs, and a description of the agency's current organization and field centers.

GENERAL ACCOUNTING OFFICE

Copies of GAO Publications are available online at www.gao.gov or by calling 202/512-6000.

- **Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research (AIMD-00-140)**
This report reviews the security of information systems that support DOE's unclassified civilian research programs. It addresses whether these systems are vulnerable to unauthorized access and what DOE is doing to address the risk.
- **Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000 (T-AIMD-00-229)**
This testimony was presented before the Subcommittee on Government Management, Information and Technology of the Committee on Government Reform. The bill is intended to remove barriers to information sharing between government and private industry in order to better address threats to the nation's critical infrastructure.
- **Clean Water Act: Proposed Revisions to EPA Regulations to Clean Up Polluted Waters (RCED-00-206R)**
This report assesses economic and compliance issues associated with two recently proposed rulemakings by the EPA. The first proposed rule would revise the total maximum daily load (TMDL) program, which is authorized by the Clean Water Act.

The second proposed rule would revise EPA's National Pollutant Discharge Elimination System (NPDES) program that controls the discharge of pollutants from "point" sources.

- **Department of Energy: National Security Controls Over Contractors Traveling to Foreign Countries Need Strengthening (RCED-00-140)**
This report describes the types of foreign-intelligence-gathering incidents that have occurred during foreign travel by contractor employees, discusses the DOE controls that apply to foreign travel by contractor employees, and identifies areas where these controls can be strengthened. The report focuses on four of DOE's nine national laboratories: Lawrence Livermore, Los Alamos, Oak Ridge, and Sandia.

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 (800/624-6242, www.nap.edu).

- **Facing the Unexpected: Disaster Preparedness and Response in the United States (ISBN: 0-309-06999-8)**
This report presents information derived from disasters around the world over the past 25 years. It explores how to improve disaster programs, identifies remaining research needs, and discusses disaster within the broader context of sustainable development. It also reviews the influences that shape the U.S. governmental system for disaster planning and response, the effectiveness of local emergency agencies, and the level of professionalism in the field.
- **From Rarity to Visibility: Gender and Career Outcomes in Science and Engineering (ISBN: 0-309-05580-6)**
This study looks at women in science and engineering careers in the 1970s and 1980s, documenting differences in career outcomes between men and women and between women of different races and ethnic backgrounds. It explores the sectors where female Ph.D.s are employed, if salary disparities exist between men and women, and how well female scientists and engineers are represented in management.
- **Marijuana As Medicine?: The Science Beyond the Controversy (ISBN: 0-309-06531-3)**
This report extracts critical findings from a recent Institute of Medicine study on the issue of utilizing marijuana for medicinal purposes. It addresses whether marijuana can relieve a variety of symptoms, the effects of its active chemical components on the immune system and on psychological health, and its potential use in comparison with existing treatments. It also answers questions about the legal status of marijuana, explaining the conflict between state and federal law regarding its medical use.

scientific definitions

1. The act of making clear and distinct.
2. the act of stating a precise meaning or significance.

ENCRYPTION Putting data into a secret code so it is unreadable except by authorized users. Types of encryption include conventional (also called private key), public key, secret key, synchronous, and symmetric.

CONVENTIONAL ENCRYPTION A form of encryption in which sender and receiver share with each other a secret key to decrypt messages sent between them. Conventional encryption, also called private key encryption, is different from public key encryption in which both sender and receiver have the public key, but each has a private key which is not shared.

PUBLIC KEY ENCRYPTION A way of encrypting messages in which each user has a public key and a private key. Messages are sent encrypted with the receiver's public key; the receiver decrypts them using the private key. Using this method, the private key never has to be revealed to anyone other than the user.

COMPUTER VIRUS A program that infects a computer by attaching itself to another program, and propagating itself when that program is executed. A computer can become infected by files downloaded over a network, or by the installation of new software or floppy disks that are infected with viruses. Some viruses are only pranks, and perform harmless actions like displaying a screen with a joke message on it. Others can destroy files or wipe out a hard drive.

WORM A computer program that can make copies of itself, and spreads through connected systems, using up resources in affected computers or causing other damage.

BIOTECHNOLOGY A set of biological techniques developed through basic research and now applied to research and product development. In particular, the use by industry of recombinant DNA, cell fusion, and new bioprocessing techniques.

HUMAN GENE THERAPY Insertion of normal DNA directly into cells to correct a genetic defect.

DNA (DEOXYRIBONUCLEIC ACID) The molecule that encodes genetic information. DNA is a double-stranded molecule held together by weak bonds between base pairs of nucleotides. The four nucleotides in DNA contain the bases: adenine (A), guanine (G), cytosine (C), and thymine (T). In nature, base pairs form only between A and T and between G and C; thus the base sequence of each single strand can be deduced from that of its partner.

RECOMBINANT DNA A DNA molecule containing DNA originating from two or more sources.

VIRAL VECTORS A virus used in genetic engineering to insert genes into a cell. Viral DNA that has been modified to serve as a vector for recombinant DNA.

Source: www.eurekaalert.org/resources/definitions.html

Cyber Security Bill... Continued from page 1

Y2K Act, H.R. 4246 contains three similar exemptions, but now it is the FOIA provision, not the liability provision, that has attracted attention.

In recent years, as the country's critical infrastructure has become more interconnected, it has also grown more vulnerable to cyber attacks. While the most damaging computer security incidents, such as the "Love Bug" virus, are widely reported in the press, thousands more occur that do not attract much attention, and there is evidence that their prevalence is increasing. The CERT Coordination Center at Carnegie Mellon University, which was established in 1988 to track and respond to cyber threats and vulnerabilities, received over 9,800 incident reports in 1999, up from 3,700 the year before. Fears have arisen that a determined individual could do great damage to the nation's economy by attacking computer networks essential to its critical infrastructure. Calls have therefore come from many different quarters to take action on cyber security.

In January, the Clinton Administration heeded these calls and mapped out the first stage of its ongoing efforts in the "National Plan for Information Systems Protection." This addressed two broad goals: tightening cyber security in the federal government and promoting public-private cyber security partnerships. To address the second goal, the plan included the creation of Information Sharing and Analysis Centers (ISACs) that would allow private sector companies and the federal government to pool information. The plan called for an ISAC for six industry sectors, each assisted by an associated federal agency.

ISACs have already been set up for the finance and telecommunications industries, and the model has been widely praised. However, some businesses have expressed reluctance to participate due to a concern that sensitive information released to an ISAC could be made public through FOIA. The Davis-Moran bill is an attempt to address this concern. At a June 22 hearing on the bill before the Subcommittee on Government Management, Information, and Technology of the House Government Reform Committee, L. Craig Johnstone of

>>> *Continued on next page*

Cyber Security Bill...

Continued from previous page

the U.S. Chamber of Commerce echoed these fears of public disclosure and praised the lawmakers' efforts: "The government can expect the amount of valuable information passed on to agencies about Inter-

"Fears of publicity, fears of inviting additional attacks, fears of confidentiality, ... have, in the past, limited the willingness of industry members to share information."

net threats and vulnerabilities to be directly proportional to the amount of safety provided by H.R. 4246. No protection, no information, plain and simple."

However, David L. Sobel, General Counsel for the Electronic Privacy Information Center (EPIC), testified that confidential cyber security information is already exempt from FOIA, under what is known as a (b)4 exemption. He emphasized the benefits of FOIA and expressed concern that the bill would erect a new barrier to obtaining information that should be disclosed. "[T]his exemption approach [of H.R. 4246] is fundamentally inconsistent with the basic premise of the FOIA," he said. Johnstone replied that the interpretation of FOIA is still open to debate. Confirming this statement was John Tritak, Director of the Critical Infrastructure Assurance Office at the Department of Commerce, who said that while the government believes existing FOIA exemptions are sufficient, there is debate about their meaning in the legal community.

In a May 5 critique posted on their website, the Center for Democracy and Technology (CDT) argues that several parts of H.R. 4246 are problematic. The organization does not explicitly describe the bill as unnecessary but does imply strong reservations about it and suggests that a more limited approach be taken that fits within the framework of the (b)4 exemption.

For example, the CDT critique objects to the use of the Y2K Act as a model for H.R. 4246, identifying major differences in the intent of the bills. While the goal of the Y2K bill was free and open disclosure, the goal of H.R. 4246 is limited, secure disclosure. H.R. 4246 is intended partly to keep terrorists from learning about the vulnerabilities of the nation's critical infrastructure. Y2K, meanwhile, "involved a known problem that was going to cause unpredictable damage unless fixed. It made no sense to hide the problem out of fear that it could be exploited by terrorists." The Y2K bill, therefore, "addressed such a different problem and from such a different perspective that it is probably not a useful model for the cyber security issue."

CDT also raises the question of what type of ISAC the legislation is intended to promote. The finance industry's ISAC, which was established last year, has avoided FOIA concerns because it only allows the federal government to disseminate information, not collect it. However, Daniel Woolley, the president of Global Integrity Corporation, which established the finance industry's ISAC, nonetheless supported H.R. 4246 at the June 22 hearing. "Fears of publicity, fears of inviting additional attacks, fears of confidentiality, ... have, in the past, limited the willingness of industry members to share information," he said. "... [L]imited legislation such as H.R. 4246, which removes barriers to information sharing, is a good idea."

H.R. 4246, which remains under consideration by the Commerce Committee and has also been referred to the Judiciary Committee, comes amid a myriad of proposed bills that relate to cyber security. For example, Sen. Orrin G. Hatch (R-UT) and Sen. Charles E. Schumer (D-NY) have proposed the Internet Integrity and Critical Infrastructure Protection Act of 2000 (S. 2448), which would expand federal prosecution of computer crimes; in February, the House passed the Wireless Privacy Enhancement Act of 1999 (H.R. 514), which is designed to combat eavesdropping on wireless communications; on July 26, the House Science Committee passed the Computer Security Enhancement Act (H.R. 2413), which would strengthen the role of the National Institute of Standards and Technology in ensuring the security of federal computer systems; and on July 17, the White House announced that it would propose legislation to update wiretapping laws. •••

FOR MORE INFORMATION:

CERT Coordination Center, Carnegie Mellon University: www.cert.org

"National Plan for Information Systems Protection": www.whitehouse.gov/WH/EOP/NSC/html/NSC_Documents.html

Electronic Privacy Information Center (EPIC): www.epic.org

U.S. Chamber of Commerce: www.uschamber.com

Center for Democracy and Technology (CDT): www.cdt.org

House Government Reform Committee: www.house.gov/reform

Science and Technology in Congress (ISSN#1096-0406) is published by the Center for Science, Technology, and Congress (CSTC) at the American Association for the Advancement of Science (AAAS). It is distributed 8 times per year: February through August and October. Issue Updates are published periodically to supplement the newsletter.

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 newsletter 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 or congress_center@aaas.org. Subscriptions are free for congressional staff; \$40 for others.

Science and Technology in Congress
AAAS

1200 New York Avenue, NW
Washington, DC 20005

Phone 202/326-6600 Fax 202/289-4950

Web www.aaas.org/spp/cstc

E-mail congress_center@aaas.org

- Albert H. Teich
Director, Science and Policy Programs
- Joanne Padrón Carney, *Director, CSTC*
- David G. Cooper, *Project Coordinator, CSTC*



AMERICAN ASSOCIATION FOR THE
ADVANCEMENT OF SCIENCE

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

Address Change Requested

Heard off the Hill

this piece of conventional wisdom. In a study of 112 college students, each participant was asked to fill out several personality questionnaires and shake hands with four "handshake coders" trained in evaluating handshakes. Those with firm handshakes were more extroverted and open to experience than those with limp handshakes; men tended to have firmer handshakes than women; and women who are more liberal, intellectual, and open to new experiences had firmer handshakes than those who were less so.

---> *Washington Post, July 9, 2000*

Martian Gullies • Cameras orbiting Mars aboard NASA's Mars Global Surveyor have captured images of Earth-like gullies that were formed by fluid flows emerging from Martian rock. Some scientists believe these flows consisted of liquid water, causing a great deal of excitement among those interested in the possibility of life on the red planet. However, other scientists argue that the surface of Mars is too cold for water to flow and suggest other mechanisms. But in either case, the discovery will likely have major implications for the geological dynamics of the red planet.

---> *Science, June 30, 2000*

Telling Handshakes • It is often said that a lot can be learned from a person's handshake. Now, psychologists at the University of Alabama have confirmed

Seeing Red • Doomsayers often tout the impending onslaught of dangerous cyber terrorists who will wreak havoc in our nation's computer systems and bring to life the system administrator's worst nightmare. But for some administrators, the Red Team at Sandia National Laboratories has already given life to such nightmares. By taking on the role of the hostile intruder, members of the Red Team expose vulnerabilities in their clients' systems and help to improve security. They adopt a wide range of hacker personality types, and mount attacks that can range from a week to five months. Two large corporations and several key government agencies have enlisted their help so far. The team's success rate? Of the 35 systems they have worked on, every one has been invaded.

---> *EurekaAlert!, July 25, 2000*

Fish Eyes • Thanks to a blind variety of cave fish found in north-eastern Mexico and a close seeing relative, biologists have gained new insight into the development of the fish's eyes. In the blind variety, which lives in dark caves and underground waterways and has evolved from the seeing variety, the eyes have become sunken into their sockets and covered over by flaps of skin. By closely monitoring the embryonic growth of the blind fish, the scientists found that a lens forms, but then degenerates, and that other eye structures, such as the cornea and iris, never form. However, when this lens is replaced by a lens from the seeing fish, it does not degenerate, and the rest of the eye develops normally. This discovery should prove significant in studying evolutionary processes.

---> *Science, July 28, 2000*