genes increase or decrease our health risks, interacting with a complex web of environmental and other factors to produce an actual health outcome.

Our understanding of genetics and the interplay between genes and outside influences is still in its infancy, but it is growing every day. The Human Genome Project, coordinated by the National Human Genome Research Institute, now predicts that we will have a "working draft" of the entire human genome by early in the year 2000. A complete, highly accurate transcript will be completed only perhaps two to three years later. In the meantime, science will continue racing ahead to identify genes associated with specific traits and diseases. Before long, new gene-based therapies will likely be available to treat genetic diseases, ushering in a new era in human medicine.

The promise of genetic research and technology seems almost limitless. Unfortunately, the potential for abuse of genetic information is also considerable. Many health insurers and employers have already expressed a keen interest in the potential to use genetic information. In some cases, this genetic information would not be used to pursue the best interests of the individuals involved. Health insurers may wish to use genetic data to determine which consumers are likely to be the most or least healthy, setting insurance premiums accordingly or denying coverage altogether. Employers could use genetic information in hiring or promotion decisions, or as a tool to keep their company's insurance premiums low. In either situation, such actions would effectively punish individuals for being born with certain genes.

Americans are deeply concerned about the possibility of genetic discrimination. In a recent poll of Better Homes & Gardens readers, fully 90 percent of respondents said they were extremely, very, or somewhat concerned when asked, "How concerned are you that [genetic] tests will be used to deny health insurance or even jobs?" Even more worrisome, evidence is emerging that many people are deciding not to participate in clinical trials or genetic research because they fear their genetic information might not remain private. Clearly, we must protect the privacy of genetic information and prevent abuse of this data if we are to avoid damaging the propsects of genetic research for curing human ills.

The Genetic Nondiscrimination in Health Insurance and Employment Act would provide all Americans with the necessary guarantees that their genetic information will not be used against them. This bill would prevent insurers from raising insurance premiums or denying coverage based on predictive genetic information. It would also prohibit insurance companies from requiring disclosure of this sensitive information or revealing it to third parties without consent. These provisions are backed up with meaningful penalties and remedies.

In addition, this bill contains crucial provisions banning genetic discrimination in employment. Under this legislation, employers would be barred from failing to hire, firing, or discriminating against workers with respect to the compensation, terms or privileges of employment based on genetic information. Employers would be prohibited from collecting genetic information except in connection with a program to monitor biological effects of toxic substances in the workplace. Finally, the privacy of genetic information would be protected by preventing employers from disclosing this information to outside parties.

I am pleased to note that companion legislation is being introduced today by Senators TOM DASCHLE, EDWARD KENNEDY, TOM HARKIN, and CHRISTOPHER DODD. Our bill is supported by a broad range of organizations active on health care issues. I look forward to building a bipartisan coalition in support of this bill, which responds effectively to the concerns of the American people with regard to genetics.

Mr. Speaker, I urge the House leadership to schedule hearings immediately on the Genetic Nondiscrimination in Health Insurance and Employment Act. With completion of the human genome mapping imminent, we cannot afford to waste any more time in addressing these critical issues. Congress must act quickly to protect all Americans against genetic discrimination and secure the future of genetic research.

HEALTH OF THE AMERICAN PEOPLE

SPEECH OF

HON. NANCY PELOSI

OF CALIFORNIA

IN THE HOUSE OF REPRESENTATIVES

Wednesday, June 30, 1999

Ms. PELOSI. Mr. Speaker, people from my district in San Francisco come to visit my office wanting to talk about their personal battle against disease. They include parents of children with juvenile diabetes, women fighting a breast cancer diagnosis, families of people with Parkinson's, and people struggling with HIV disease and AIDS.

They come to talk about different problems, but speak with one resounding voice about how they want Congress to respond. Their message to me, and to all of us, is that funding for the National Institutes of Health must be doubled over five years.

My colleagues, we must heed their message and continue to increase NIH funding to achieve this goal. As a member of the Appropriations Subcommittee on Labor-HHS-Education, I strongly supported last year's $2 billion, or 15%, increase in the research budget at the NIH, bringing total funding to $15.6 billion. And this year, I am an original cosponsor of H. Res. 89, legislation that expresses the sense of the House of Representatives that NIH funding should be increased by another $2 billion in fiscal year 2000.

I support these increases because I believe we are on the verge of making great leaps ahead in our ability to treat and prevent a wide range of diseases. Dr. Harold Varmus, Director of NIH, has testified before the Labor-HHS-Education Subcommittee that, "discoveries are occurring at an unprecedented pace in biology and medicine, presaging revolutionary changes in medical practice during the next decade." We have a responsibility to take advantage of this enormous opportunity to advance science, fight disease, and save and prolong life.

There are many success stories to point to at NIH and many challenges that lie ahead, including eliminating health disparities, reinvigorating clinical research, finding cures and vaccines for hundreds of diseases including malaria, cancer and HIV, and mapping the human genome and making in accessible to scientists across the world.

As Dr. Varmus testified this year, "Throughout the world, the NIH is considered the leading force in mankind's continuing war against disease." Our wise investment in NIH is paying off. We must enter the new millennium investing in science that can unlock secrets of human disease and human health, and change our world for the better. I urge my colleagues to support a doubling in NIH funding over five years.

INTRODUCTION OF H.R. 2413, THE COMPUTER SECURITY ENHANCEMENT ACT OF 1999

HON. F. JAMES SENSENBRENNER, JR.

OF WISCONSIN

IN THE HOUSE OF REPRESENTATIVES

Thursday, July 1, 1999

Mr. SENSENBRENNER. Mr. Speaker, I am pleased to introduce, H.R. 2413, the Computer Security Enhancement Act of 1999, a bipartisan bill to address our government's computer security needs. Joining me as cosponsors of this important legislation is Mr. Bart Gordon of Tennessee and Mrs. Connie Morella of Maryland, the Chairwoman of the Science Committee's Technology Subcommittee.

The bill amends and updates the Computer Security Act of 1987 which gave the National Institute of Standards and Technology (NIST) the lead responsibility for developing security standards and technical guidelines for civilian government agencies' computer security. Specifically, the bill:

1. Reduces the cost and improves the availability of computer security technologies for Federal agencies by requiring NIST to promote the Federal use of off-the-shelf products for meeting civilian agency computer security needs.

2. Enhances the role of the independent Computer System Security and Privacy Advisory Board in NIST's decision-making process. The board, which is made up of representatives from industry, federal agencies and other outside experts, should assist NIST in its development of standards and guidelines for Federal systems.

3. Requires NIST to develop standardized tests and procedures to evaluate the strength of foreign encryption products. Through such tests and procedures, NIST, with assistance from the private sector, will be able to judge the relative strength of foreign encryption, thereby defusing some of the concerns associated with the expert of domestic encryption products.

4. Clarifies that NIST standards and guidelines are to be used for the acquisition of security technologies for the Federal Government and are not intended as restrictions on the production or use of encryption by the private sector.

5. Addresses the shortage of university students studying computer security. Of the 5,500 PhDs in Computer science awarded over the last five years in Canada and the U.S., only 16 were in fields related to computer security. To help address such shortfalls, the bill establishes a new computer science fellowship program for graduate and undergraduate students studying computer security; and

6. Requires the National Research Council to conduct a study to assess the desirability of creating public key infrastructures. The study will also address advances in technology required for public key in technology required for public key infrastructure.

7. Establishes a national panel for the purpose of exploring all relevant factors associated with the development of a national digital signature infrastructure based on uniform standards and of developing model practices and standards associated with certification authorities.

All these measures are intended to accomplish two goals. First, assist NIST in meeting the ever-increasing computer security needs of Federal civilian agencies. Second, to allow the Federal Government, through NIST, to harness the ingenuity of the private sector to help address its computer security needs.

Since the passage of the Computer Security Act, the networking revolution has improved the ability of Federal agencies to process and transfer data. It has also made that same data more vulnerable to corruption and theft.

The General Accounting Office (GAO) has highlighted computer security as a government-wide, high-risk issue. GAO specifically identified the lack of adequate security for Federal civilian computer systems as a significant problem. Since June of 1993, the General Accounting Office (GAO) has issued over 30 reports detailing serious information security weaknesses at 24 of our largest Federal agencies.

The Science Committee has held seven hearings on computer security since I became Chairman in 1997. During the hearings, Members of the Science Committee heard from some of the most respected experts in the field. They all agreed that the Federal Government must do more to secure the sensitive electronic data it possesses.

The Federal Government is not alone in its need to secure electronic information. The corruption of electronic data threatens every sector of our economy. The market for high-quality computer security products is enormous, and the U.S. software and hardware industries are responding. The passage of this legislation will enable the Federal Government, through NIST, to benefit from these technological advances.

I look forward to working with all interested parties to advance the Computer Security Enhancement Act of 1999. In my estimation, it is a good bill, and I am hopeful we can move it through the legislative process in short order.

THE COMPUTER SECURITY ENHANCEMENT ACT OF 1999

HON. BART GORDON

OF TENNESSEE

IN THE HOUSE OF REPRESENTATIVES

Thursday, July 1, 1999

Mr. GORDON. Mr. Speaker, today, I am pleased to join Chairman SENSENBRENNER in introducing the Computer Security Enhancement Act of 1999. I was an original co-sponsor of similar legislation in the 105th Congress. The measure follows a stream of attacks just this past week on government Web sites including the Senate, White House, the National Oceanic Atmospheric Administration's severe weather warning site, the Defense Department and the FBI's National Infrastructure Protection Center, whose very purpose is to protect federal sites from such attacks.

The Computer Security Enhancement Act of 1999 will encourage the use of computer security products, both by federal agencies and the private sector, which in turn will support the new electronic economy. I am convinced that we must have trustworthy and secure electronic network systems to foster the growth of electronic commerce. This legislation builds upon the successful track record of the National Institute of Standards and Technology (NIST) in working with industry and other federal agencies to develop a consensus on the necessary standards and protocols required to support electronic commerce.

Chairman SENSENBRENNER has already outlined the provisions of this bill. However, I would like to take a few minutes to explain provisions I added to this legislation that are based on H.R. 1572, the Digital Signature Act of 1999, which I introduced with the support of Chairman SENSENBRENNER on 27 April 1999 to complement last year's Government Paperwork Elimination Act. When I introduced H.R. 1572, I stated that it was a work in progress. Section 13 of the Computer Security Enhancement Act, which we are introducing today, is the result of discussions I have had with industry and federal agencies.

As a result of these discussions, the general provisions in H.R. 1572 have been re-drafted to include all electronic authentication techniques. Section 13 requires NIST, working with industry, to develop minimum technical standards and guidelines for Federal agencies to follow when deploying any electronic authentication technologies. In addition, Section 13 authorizes the Undersecretary of Commerce for Technology to establish a National Policy Panel for Digital Signatures to explore the factors associated with the development of a National Digital Signature Infrastructure based on uniform model guidelines and standards to enable the widespread utilization of digital signatures in the private sector.

I want to highlight that these provisions are technology neutral. Rather they encourage federal agencies to use uniform guidelines and criteria in deploying electronic authentication technologies and to ensure that their systems are interoperable. The provisions also encourage agencies to use commercial off-the-shelf software (COTS) whenever possible to meet their needs. None of these provisions give the Federal government the authority to establish standards or procedures for the private sector.

The use of electronic authentication technologies are critical for the continued growth and security of electronic transactions on the Internet. With the rapid growth of the Internet we have lost the ability to actually "know" who we are communicating with is who they say they are. In order to exchange sensitive documents or to do business transactions with confidence it is important that electronic authentication systems are used that both uniquely identify both the sender and/or the recipient and verify that the information exchanged has not been altered in transit. Electronic authentication is as much of a computer security issue as having good firewalls, strong encryption, and virus scanners.

I want to stress the underlying principle of the Computer Security Enhancement Act of 1999 is that it recognizes that government and private sector computer security needs are similar. Hopefully the result will be greater security and lower cost for everyone as we increasingly move towards an electronic economy.

The bill we are introducing today is the result of close bipartisan cooperation and it has been a pleasure working with Chairman SENSENBRENNER on this legislation.

I urge my colleagues to support the Computer Security Enhancement Act of 1999.

EDUCATIONAL TECHNOLOGY UTILIZATION EXTENSION ASSISTANCE ACT

HON. JAMES A. BARCIA

OF MICHIGAN

IN THE HOUSE OF REPRESENTATIVES

Thursday, July 1, 1999

Mr. BARCIA. Mr. Speaker, I am pleased to introduce, along with my friend from Oregon, Mr. Wu, the Educational Technology Utilization Extension Assistance Act. This bill directs the National Science Foundation to work with the Department of Education and the National Institute of Standards and Technology to create educational technology extension centers based at undergraduate institutions. The focus of these centers is to advise and assist local K–12 schools to better utilize and integrate their existing ed-tech infrastructure into their curriculum and classroom.

During my tenure in Congress, much attention has been given to the subject of computers in the classroom and wiring schools for the Internet. These initiatives are often viewed as a panacea for improving test scores, and millions of dollars have been invested in these technologies. Missing from this strategy is any useful, long-term advice on how to best integrate ed-tech into the educational process. In fact, one of the last reports produced by the excellent staff of OTA highlighted the problem of teachers not being effectively trained on how to best use these technologies in the classroom. The same report pointed out that local school officials were often unaware of the substantial infrastructure and operational costs associated with deploying and maintaining these educational technologies.

These findings were echoed by a February 1999 Department of Education report, "Teacher Quality: A Report on the Preparation and Qualification of Public School Teachers." The Department of Education found that only 1 in 5 teachers felt well-prepared to work in a modern classroom. In addition, the most common form of professional development for K–12 teachers are 1-day workshops which have little relevance to classroom activities. Consequently, the full potential of ed-tech has never been fully realized.

The Educational Technology Utilization Assistance Act is an attempt to rectify this gap in the educational infrastructure. This bill does not create a new top-down Federal program, but rather it allows local extension centers to assist local primary schools to better integrate educational technologies into their curriculum. Of course this concept is not new. In fact, it is based on the highly successful Agricultural Extension Service and the Manufacturing Extension Partnership. Both of these programs are model public/private partnerships that use specific solutions to solve unique problems as they are found in the field and rejects the "one

Document No. 87