

of this House is preventing us from getting votes on three amendments: one to ensure that our friends in New York get the relief they were promised 2 months ago; the second to make certain that we increase the Pentagon budget in areas thought necessary; and, third, to increase our homeland security.

Mr. Speaker, I urge the leadership of this House to allow us to vote on those three amendments. They do not need to vote for them, just allow us to vote on them.

There was an amendment today offered on New York which purports to take care of those problems. With all due respect, in my view, any Member of the New York delegation who tries to walk around in public using that as a fig leaf would be arrested for indecent exposure because that amendment does virtually nothing. It gives no political cover; and it should not, because it provides no substantive improvement.

I urge the House to allow us to vote on those three amendments. This involves the national security of the United States. We should not be operating under a gag rule. We should not be relying on a traffic cone as a major deterrent on the Canadian border, and that is what we will be doing without the amendment that we want to vote on when we return.

---

#### FURTHER MESSAGE FROM THE SENATE

A further message from the Senate by Mr. Monahan, one of its clerks, announced that the Senate has passed a bill of the following title in which the concurrence of the House is requested:

S. Con. Res. 85. Concurrent resolution providing for a conditional adjournment or recess of the Senate and a conditional adjournment of the House of Representatives.

---

The SPEAKER pro tempore (Mr. OTTER). Under a previous order of the House, the gentlewoman from Texas (Ms. JACKSON-LEE) is recognized for 5 minutes.

(Ms. JACKSON-LEE addressed the House. Her remarks will appear hereafter in the Extensions of Remarks.)

---

#### COMPUTER SECURITY ENHANCEMENT AND RESEARCH ACT OF 2001

The SPEAKER pro tempore. Under a previous order of the House, the gentleman from Washington (Mr. BAIRD) is recognized for 5 minutes.

Mr. BAIRD. Mr. Speaker, today I am introducing the Computer Security Enhancement and Research Act of 2001. This legislation will address the long-term needs in securing our Nation's information infrastructure and will strengthen the security of the non-classified computer systems of Federal agencies. The bill establishes a research and development program on computer and network security at the

National Institute of Standards and Technology. It also strengthens the institute's existing responsibilities in developing best computer security practices and standards in assisting Federal agencies to implement effective computer and network security.

Because of the September 11 tragedy, attention is now focused in an unprecedented way on increasing our security against terrorism. Our concerns include protecting critical national infrastructures. Today, security has to mean more than locking doors or guarding buildings and installing metal detectors.

In addition to physical security, virtual systems that are vital to our Nation's economy must be protected. Telecommunications and computer technologies are vulnerable to attack from far away by enemies who can remain anonymous, hidden in the vast maze of the Internet. Examples of systems that rely on computer networks include the electric power grid, rail networks, and financial transaction networks. Just as enemies are achieving a sophistication to use the most complex weapons against us, our vital computer networks have become more interconnected and more accessible and, therefore, more vulnerable via the Internet.

The vulnerability of the Internet to computer viruses, denial-of-service attacks, and defaced Web sites is well known. These widely reported events have increased in frequency over time. These attacks disrupt business and government activities sometimes resulting in significant economic recovery costs. While no catastrophic cyberattack has occurred thus far, Richard Clarke, the President's new cyberterrorism czar, has said that the Government must make cybersecurity a priority or face, in his words, the possibility of a digital Pearl Harbor.

While potentially vulnerable computer systems are largely owned and operated by the private sector, the Government has an important role in supporting the research and development activities that will provide the tools for protecting information systems. An essential component for ensuring improved information security is a vigorous and creative research program focused on the security of networked information systems. Unfortunately, witnesses at a recent Committee on Science and Technology hearing indicated that current R&D efforts fall far short of what is required.

Witnesses at that hearing noted the anemic level of funding for research on computer and network security. This lack of funding has resulted in the lack of critical mass of researchers in the field and a lack of focus on safe, incremental research projects. The witnesses advocated increased and sustained research funding from a Federal agency assigned the role to support such research on a long-term basis. To date, Federal support for computer security research has been directed at de-

fense and intelligence needs. While this work on encryption and defense systems security protocols are absolutely vital, very little has been done on the civilian side of communications security.

The bill I am introducing explicitly addresses this gap in Federal support for computer security. My bill charges the National Institute of Standards and Technology with implementing a substantial program of research support based at institutions of higher education designed to improve the security of networked information systems. The research program is authorized for a 10-year period, growing from \$25 million in the first year to \$85 million in the fifth year. This may sound like a substantial amount of money, but the billions of dollars that are lost in successful computer attacks makes this paltry by comparison. Although the award would go to universities, the research projects may involve collaboration with for-profit companies that develop information security products.

The bill establishes a flexible management approach for the research program. It is based upon management style that has been used effectively by DARPA, the Defense Advanced Research Projects Agency, to spur advances in high technology fields. Specifically, management of the research program will rely on program managers who are both knowledgeable about computer security issues and needs and familiar with the research community. These program managers will be responsible for identifying and nurturing talented researchers and for generating innovative research proposals. Although program managers will have considerable freedom in managing their individual research portfolios, each will be reviewed periodically by NIST senior managers and by outside computer security experts. To ensure its relevance and continued need of this program, it will be reviewed in its fifth year for scientific merit and relevance by the National Academy of Sciences.

An expanded university-based research program will train new graduate students as well as postdoctoral research assistants, as well as attracting seasoned researchers to the field. The result will be a larger and more vibrant basic research enterprise in computer-related security fields. A separate set of awards will be available to support postdoctoral research fellowships and senior research fellowships both at universities and at NIST. The bill also increases support for ongoing, in-house computer security at NIST.

The Computer Security Enhancement and Research Act of 2001 builds on the long experience of NIST in developing computer security standards and practices by placing new responsibilities on the agency for building up the Nation's basic research enterprise in information security. By enlarging and strengthening the research enterprise, we can generate the ideas, approaches, and technologies needed to