Brown (OH)	Gutknecht	Menendez
Brown (SC)	Hall (TX)	Mica
Bryant	Hansen	Millender-McDonald
Buyer	Harman	Miller, Dan
Callahan	Hart	Miller, Gary
Calvert	Hastings (FL)	Miller, George
Camp	Hastings (WA)	Miller, Jeff
Cannon	Hayes	Mink
Cantor	Hayworth	Mollohan
Capito	Hefley	Moran (KS)
Capps	Herger	Moran (VA)
Cardin	Hill	Morella
Carson (IN)	Hilliard	Murtha
Carson (OK)	Hinchey	Myrick
Castle	Hinojosa	Nadler
Chabot	Hobson	Napolitano
Chambliss	Hoeffel	Neal
Clayton	Hoekstra	Nethercutt
Clement	Holden	Ney
Clyburn	Holt	Norwood
Coble	Honda	Nussle
Collins	Hooley	Oberstar
Combest	Horn	Olver
Condit	Hostettler	Ortiz
Conyers	Houghton	Osborne
Cooksey	Hoyer	Ose
Costello	Hulshof	Otter
Cox	Hunter	Owens
Coyne	Inslee	Oxley
Cramer	Isakson	Pallone
Crane	Israel	Pascrell
Crenshaw	Issa	Pastor
Crowley	Istook	Paul
Culberson	Jackson (IL)	Payne
Cummings	Jackson-Lee (TX)	Pelosi
Cunningham	Jenkins	Pence
Davis (CA)	John	Peterson (MN)
Davis (FL)	Johnson (CT)	Peterson (PA)
Davis (IL)	Johnson (IL)	Petri
Davis, Jo Ann	Johnson, E. B.	Phelps
Davis, Tom	Johnson, Sam	Pickering
Deal	Jones (NC)	Platts
DeFazio	Jones (OH)	Pombo
DeGette	Kanjorski	Pomeroy
Delahunt	Keller	Portman
DeLauro	Kelly	Price (NC)
DeLay	Kennedy (MN)	Pryce (OH)
DeMint	Kennedy (RI)	Putnam
Deutsch	Kerns	Quinn
Diaz-Balart	Kildee	Radanovich
Dicks	Kilpatrick	Rahall
Dingell	Kind (WI)	Ramstad
Doggett	King (NY)	Rangel
Dooley	Kingston	Regula
Doolittle	Kirk	Rehberg
Doyle	Knollenberg	Reyes
Dreier	Kolbe	Reynolds
Duncan	Kucinich	Rivers
Dunn	LaFalce	Rodriguez
Edwards	LaHood	Roemer
Ehlers	Lampson	Rogers (KY)
Ehrlich	Langevin	Rogers (MI)
Emerson	Lantos	Rohrabacher
Engel	Larsen (WA)	Ros-Lehtinen
English	Larson (CT)	Ross
Eshoo	Latham	Rothman
Etheridge	LaTourette	Roybal-Allard
Everett	Leach	Royce
Farr	Lee	Rush
Ferguson	Levin	Ryun (KS)
Filner	Lewis (CA)	Sabo
Flake	Lewis (GA)	Sanchez
Fletcher	Lewis (KY)	Sanders
Foley	Lipinski	Sandlin
Forbes	LoBiondo	Sawyer
Ford	Lofgren	Saxton
Fossella	Lowey	Schaffer
Frank	Lucas (KY)	Schakowsky
Frost	Lynch	Schiff
Gallegly	Maloney (CT)	Schrock
Ganske	Manzullo	Scott
Gekas	Markey	Sensenbrenner
Gephardt	Mascara	Serrano
Gibbons	Matheson	Sessions
Gilchrest	Matsui	Shadegg
Gillmor	McCarthy (MO)	Shays
Gilman	McCarthy (NY)	Sherman
Gonzalez	McCollum	Sherwood
Goodlatte	McCrery	Shimkus
Gordon	McGovern	Shows
Goss	McHugh	Shuster
Graham	McInnis	Simmons
Granger	McIntyre	Simpson
Graves	McKeon	Skeen
Green (TX)	McNulty	Skelton
Green (WI)	Meehan	Smith (MI)
Greenwood	Meek (FL)	Smith (NJ)
Grucci	Meeks (NY)	Smith (TX)
Gutierrez		
Smith (WA)	Thomas	Walsh
Snyder	Thompson (CA)	Wamp
Solis	Thompson (MS)	Watkins (OK)
Souder	Thornberry	Watson (CA)
Spratt	Thune	Watt (NC)
Stark	Thurman	Watts (OK)
Stearns	Tiahrt	Waxman
Stenholm	Tiberi	Weiner
Strickland	Tierney	Weller
Stump	Toomey	Wexler
Stupak	Towns	Wicker
Sununu	Turner	Wilson (SC)
Sweeney	Udall (CO)	Wolf
Tancredo	Udall (NM)	Woolsey
Tanner	Upton	Wu
Tauscher	Velazquez	Wynn
Taylor (MS)	Visclosky	Young (FL)
Taylor (NC)	Vitter	
Terry	Walden	

NOT VOTING—43

Barton	Hyde	Riley
Blagojevich	Jefferson	Roukema
Bono	Kaptur	Ryan (WI)
Burr	Kleczka	Shaw
Burton	Largent	Slaughter
Capuano	Linder	Tauzin
Clay	Lucas (OK)	Traficant
Cubin	Luther	Waters
Evans	Maloney (NY)	Weldon (FL)
Fattah	McDermott	Weldon (PA)
Frelinghuysen	McKinney	Whitfield
Goode	Moore	Wilson (NM)
Hall (OH)	Northup	Young (AK)
Hastert	Obey	
Hilleary	Pitts	

□ 1047

So the resolution was agreed to.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

Stated for:

Mr. BARTON of Texas. Mr. Speaker, on roll-call No. 12 I was inadvertently detained. Had I been present, I would have voted "yea."

MESSAGE FROM THE SENATE

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

H.R. 586. An act to amend the Internal Revenue Code of 1986 to provide that the exclusion from gross income for foster care payments shall also apply to payments by qualified placement agencies, and for other purposes.

The message also announced that the Senate has passed without amendment in which the concurrence of the House is requested, a joint resolution of the House of the following title:

H.J. Res. 82. Joint resolution recognizing the 91st birthday of Ronald Reagan.

The message also announced that the Senate has passed bills of the following titles in which the concurrence of the House is requested:

S. 1274. An act to amend the Public Health Service Act to provide programs for the prevention, treatment, and rehabilitation of stroke.

S. 1275. An act to amend the Public Health Service Act to provide grants for public access defibrillation programs and public access defibrillation demonstration projects, and for other purposes.

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT

The SPEAKER pro tempore (Mr. SHIMKUS). Pursuant to House Resolution 343 and rule XVIII, the Chair declares the House in the Committee of the Whole House on the State of the Union for the consideration of the bill, H.R. 3394.

□ 1048

IN THE COMMITTEE OF THE WHOLE

Accordingly, the House resolved itself into the Committee of the Whole House on the State of the Union for the consideration of the bill (H.R. 3394) to authorize funding for computer and network security research and development and research fellowship programs, and for other purposes, with Mr. SUNUNU in the chair.

The Clerk read the title of the bill.

The CHAIRMAN. Pursuant to the rule, the bill is considered as having been read the first time.

Under the rule, the gentleman from New York (Mr. BOEHLERT) and the gentleman from Texas (Mr. HALL) each will control 30 minutes.

The Chair recognizes the gentleman from New York (Mr. BOEHLERT).

GENERAL LEAVE

Mr. BOEHLERT. Mr. Chairman, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and to include extraneous material on H.R. 3394.

The CHAIRMAN. Is there objection to the request of the gentleman from New York?

There was no objection.

Mr. BOEHLERT. Mr. Chairman, I yield myself such time as I may consume.

Mr. Chairman, I am honored to bring H.R. 3349, The Cyber Security Research and Development Act, before the House. Like other congressional responses to terrorism, this is a bipartisan bill. I want especially to thank our ranking minority member, the gentleman from Texas (Mr. HALL), who joined me in introducing this bill; the gentleman from Washington (Mr. Baird), whose own legislation is incorporated in H.R. 3394; the gentleman from Michigan (Mr. SMITH) and the gentleman from Michigan (Dr. EHLERS) who chair the subcommittee with jurisdiction over this bill, and their ranking members, the gentlewoman from Texas (Ms. JOHNSON) and the gentleman from Michigan (Mr. BARCIA).

Also, I would be remiss if I did not thank Dr. Bill Wulf, the president of the National Academy of Engineering and one of the Nation's leading computer scientists, whose ideas were the inspiration for so much of this legislation.

I am convinced that over time H.R. 3394 will come to be seen as a fundamental turning point in the Nation's approach to cybersecurity. This bill is the equivalent of legislation the Congress passed in the wake of the Sputnik launch in the late 1950s.

We will recall that the unexpected Soviet launch of the Sputnik forced us to focus on the Nation's deficiencies in science and led us to pass breathtaking, and, it turned out, overwhelmingly effective legislation to improve

the Nation's ability to conduct research and educate students.

Similarly, the attacks of September 11 have turned our attention to the Nation's weaknesses, and, again, we find our capacity to conduct research and to educate will have to be enhanced if we are to counter our foes over the long run. No less than the Cold War, the war against terrorism will have to be waged in the laboratory as well as on the battlefield.

And I would add that I am pleased that the Committee on Science, which was created in response to the Sputnik launch, will help lead the effort to ensure our Nation's laboratories are up to the challenge.

One of the most critical problems our Nation's researchers need to focus on is how to protect our Nation's computers systems and networks from attack. For a while, most Americans have been focused exclusively on the hijackings and the bombings and bioterrorism. The experts tell us that the Nation is also profoundly at risk from cyber terrorism. That is a new word that has entered our vocabulary, unfortunately, but it is one we have to be constantly aware of, and we have to prepare.

In an era when virtually all the tools of our daily lives are connected to and rely upon computer networks, a cyberattack could knock out electricity, drinking water and sewage systems, financial institutions, assembly lines and communications, and that is just naming a few. We must improve our ability to respond to these threats, and our response must go beyond immediate defensive measures. That is not good enough.

We need to conduct the research and development necessary to make computers and networks much harder to break into and much less subject to damage when they are violated. That will require a focused, well-funded research and development effort in cybersecurity, something we are sorely lacking now.

In fact, expert witnesses at our Committee on Science hearings have described the current state of cyber security research as woefully underfunded, understaffed, timid, unimaginative and leaderless. That is not good enough. H.R. 3394 will change all of that.

Our bill capitalizes on the expertise of two well-run Federal agencies with historic links to both academia and industry necessary to jump-start our cybersecurity efforts.

Under the bill the National Science Foundation will fund the creation of new cybersecurity research centers, undergraduate and master's degree programs and graduate fellowships. The National Institute of Standards and Technology will create new program grant for partnerships between academia and industry, new postdoctoral fellowships and a new program to encourage senior researchers in other fields to work on computer security.

The result over the next several years will be to promote new research that produces innovative, creative approaches to computer security, to draw more researchers into the field, and to develop a cadre of students who will become the next generation of cybersecurity researchers.

This approach is measured and targeted, and it will be successful. As with the programs that were created in response to Sputnik, the programs in H.R. 3394 will ensure that we make the long-term investment in research and students needed to develop the tools that will protect us from cyberattacks.

I want to emphasize, Mr. Chairman, that this bill will provide funding for a wide range of research, a range far larger even than the illustrative list that is even in the legislation. For example, research would include work on firewall and antivirus technology, vulnerability assessment, operations and control systems management, and management of the interoperable digital certificates.

I also want to note that in addition to providing funding and programming, this bill provides Federal leadership. The National Science Foundation will have the responsibility of making sure that the Nation's overall research and education enterprise is producing the knowledge in students we need to combat cyberterrorism.

I have been asked by some, ''Cannot the private sector just take care of this?'' Unfortunately, the answer is a resounding no. Even after September 11, the private sector has little incentive to invest heavily in cybersecurity because the market is more concerned with speed and convenience. That is not my personal conclusion, that is what the industry leaders in cybersecurity have said in testimony before our committee.

In addition, we need to invest in our universities which will work with private industry to do the basic research needed to come up with radically new approaches to protecting our computer systems and to attract the students who will keep the field healthy in the future.

That is why H.R. 3394 is endorsed by leading industry groups including the National Association of Manufacturers, and the Information Technology Association of America, as well as a wide range of groups representing educational institutions.

The bill, I am pleased to report, is also supported by the administration, which provided much guidance as H.R. 3394 moved through our committee.

So I urge my colleagues to follow the lead of the Committee on Science, which approved this bill without dissent. Years from now we will see H.R. 3394 as the measure that galvanized the Federal Government, industry and academia into eliminating the cybersecurity weaknesses that today threaten our economy and our basic public services. I urge support for this important bill.

Mr. Chairman, I reserve the balance of my time.

Mr. HALL of Texas. Mr. Chairman, I yield myself such time as I may consume.

(Mr. HALL of Texas asked and was given permission to revise and extend his remarks.)

Mr. HALL of Texas. Mr. Chairman, I rise in support of the Cyber Security Research and Development Act. It is a bill that committee has worked in a bipartisan manner, and I think it fills a very important gap in current information technology research programs, namely the need for improved security for our computers and digital communication networks.

I, of course, congratulate and thank the Committee on Science chairman, the gentleman from New York (Mr. BOEHLERT). He has done a very good job of laying out the thrust of the bill, and I also thank him for his leadership and thank him for working so closely with me and with others on our side of the dock to bring this bill to this stage.

I also want to acknowledge the work of my colleague, the gentleman from Washington (Mr. BAIRD), a clinical psychologist before he came to the Congress, a man that has unusual ability and is knowledgeable about research and development. Actually, it was a provision pertaining to the National Institute of Standards and Technology, his provisions that originated in his bill, that we have used in this bill.

Many systems that are vital to the Nation such as electric power grids, transportation and financial services, all of these rely on the transfer of information through computer networks.

□ 1100

The trend in recent years of interconnecting computer networks has had some unintended consequences, one of them being making access of these very critical systems easier for criminals and actually potentially easier for terrorists, and that is something that we are very aware of today.

As a result, there have been an increased number of assaults on network systems. Computer viruses, attacks by computer hackers, and electronic identification theft have become more common. The events of last fall, as the chairman stated, have made us all realize just how vulnerable we are to attack, and we now understand that we have to enhance the protection of the Nation's physical and electronic infrastructure.

Mr. Chairman, H.R. 3394 establishes substantial new research programs also at the National Science Foundation and the National Institute of Standards and Technology. The goal of both of these multiyear programs is not only to advance computer security research but also to expand the community of computer security researchers.

These programs will support graduate students. They will support postdoctoral researchers and senior researchers while encouraging stronger ties between universities and industry.

The key to ensure information security for the long term is to establish a

vigorous and creative basic research effort focused on the security of networked information systems. H.R. 3394 will make a major contribution toward accomplishing this goal.

Mr. Chairman, I commend this measure to my colleagues and ask for their support and ask for its passage by this House.

Mr. Chairman, I reserve the balance of my time.

Mr. BOEHLERT. Mr. Chairman, I am pleased to yield 3 minutes to the distinguished gentleman from Michigan (Mr. SMITH), who is the chairman of the Subcommittee on Research of the Committee on Science and has been a leader in this overall effort.

Mr. SMITH of Michigan. Mr. Chairman, we learned from the September 11 attack and from the information gathered in Afghanistan to expect the unexpected.

Part of the new commitment to homeland security is improving the security of our Nation's computer and networking infrastructure. In the past decade this networking has been firmly embedded in our economy, and we have become more dependent on these technologies. Whether it is delivering agricultural products or supporting banking and financial markets, moving electricity along interconnected grids, providing government services or maintaining our national defense, we have become dependent on computer networks for our economic and national security.

The networks I think also are a potent symbol of our open society and free markets which thrive on the uninhibited flow of information. However, the technological advancement in computers and software and the networking and information technology which is a bill, H.R. 3400, which is coming before this body in the next several weeks, the potential threat of cyberattack is real and growing. Terrorists will always probe for our weakest points, so we must remain vigilant and confront these new realities.

As we become even more dependent on computer networks and as terrorists become more technologically sophisticated, we should anticipate the possibility of attacks launched on cyberspace.

Computer viruses, computer hackers, electronic identification theft are just a few of the new challenges we face. What is needed is this bill, which moves us into a comprehensive plan to address the growing linkages between national security and cybersecurity. We need to engage the best minds in America to make us immune from these kinds of attacks.

H.R. 3394 does just that. It authorizes research programs at the National Science Foundation and the National Institute of Standards and Technology to decrease the vulnerability of our computer systems and address emergency problems related to computer networking and infrastructure.

Mr. Chairman, I think it is very important that we have coordination among all government agencies in this effort, especially the military complex, if we are to be efficient, effective and if we are to succeed.

We need this kind of legislation to move ahead; and I just want to commend the gentleman from Texas (Mr. HALL), and certainly our chairman, for the inspiration to timely move this bill forward; and I urge all my colleagues to support it.

Mr. HALL of Texas. Mr. Chairman, I yield the balance of my time to the gentleman from Washington (Mr. BAIRD), for purposes of control.

The CHAIRMAN. Without objection, the gentleman from Washington (Mr. BAIRD) will control the time.

There was no objection.

Mr. BAIRD. Mr. Chairman, I yield myself such time as I may consume.

I would like to begin by commending and thanking the gentleman from New York (Mr. BOEHLERT) and the gentleman from Texas (Mr. HALL) for their leadership on this matter. I am tremendously honored that they have chosen to include my computer security bill, which establishes a research and development program on computer and network security grants to the National Institute of Standards and Technology in today's bill.

The chairman's legislation will address long-term needs in securing the Nation's information infrastructure as well as securing or strengthening the security of the nonclassified computer systems of Federal agencies.

Because of September 11, focus and attention has been focused in an unprecedented way on increasing our security against terrorism. Today, security has to mean more than locking doors and installing metal detectors. In addition to physical security, virtual systems that are vital to the 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.

I should commend the gentleman from New York (Mr. BOEHLERT), particularly, and former chair of the committee, the gentlewoman from Maryland (Mrs. MORELLA), for their foresight in this because prior to September 11 they had both had the foresight to conduct numerous hearings on the issue of computer security. It is that kind of forward thinking that we need and now in the post-September 11 time have the opportunity to implement some of these measures that came forward in those hearings.

The vulnerability of the Internet computer viruses, denial of service attacks and defaced Web sites is well-known to the general public. Such widely reported and indeed widely experienced events have increased in frequency over time. These attacks disrupt business and government activities, sometimes resulting in significant recovery costs. We have yet to face a catastrophic cyberattack thus far; but Richard Clarke, the President's new terrorism czar, has said that the government must make cybersecurity a priority or we face the possibility of what he termed a ''digital Pearl Harbor.''

Potentially vulnerable computer systems are largely owned and operated by the private sector, but 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 basic research effort focused on the security of networked information systems.

Witnesses at our Committee on Science hearings last year noted the anemic level of funding for research on computer and network security. Such lack of funding has resulted in the lack of a critical mass of researchers in the field and has severely limited the focus of research. The witnesses at the hearings advocated increased and sustained research funding from the Federal Government to support both expanded training and research on a long-term basis.

The chairman's bill will provide the resources necessary to ensure the security of business networks and the safety of America's computer infrastructure. I would like to thank the staff of the Committee on Science for their good work on this, as well as my own staff member, Brooke Jamison. I would urge all Members to support this important measure.

Mr. Chairman, I reserve the balance of my time.

Mr. BOEHLERT. Mr. Chairman, I am pleased to yield 3 minutes to the distinguished gentleman from Michigan (Mr. EHLERS), a scientist in his own right and a legislator of the first order. He is the chair of our key Subcommittee on Environment, Technology and Standards; and I am pleased to yield the time to him.

(Mr. EHLERS asked and was given permission to revise and extend his remarks.)

Mr. EHLERS. Mr. Chairman, I appreciate this opportunity to rise in support of H.R. 3394, a piece of legislation that is badly needed.

Most of the citizens of this land do not understand the broad dimensions of the problems of cybersecurity. I was privileged a few years ago to write a report for the cybersecurity of NATO parliamentary assembly but which was under the chairmanship of the gentleman from New York (Mr. BOEHLERT) at that time, and it was a real eye-opener to look into all of the dimensions of cybersecurity, both hardware and software.

On the hardware end, we are extremely vulnerable as a Nation in many ways, particularly to a high-level nuclear explosion, which would probably have no direct casualties but

could wipe out most of the computers and microprocessors in this Nation.

This bill addresses primarily the other dimension of security and that is the software problem. We have been very fortunate as a Nation that most of the breaches of security that have taken place so far have been caused by hackers, pranksters and petty thieves; but we are extremely vulnerable in many other ways due to the proliferation of computers in our country, and I am not referring just to the proliferation of microprocessors which have essentially invaded our homes, our businesses in numerous quantities. They are vulnerable in different ways; but any time one attaches a computer to a network, they are vulnerable to activities that take place on that network.

We have gained tremendously as a Nation through the use of computers and networks, but we have not taken account of the tremendous opportunities for breaches of security. It is essential that we train our people to deal with these; but above all, we must begin by doing more research in how we can deal with breaches of security. We know so little about it that we are at a disadvantage and we are at the mercy of the hackers, the pranksters, the thieves and, indeed, of other countries.

It is essential that this bill pass; that we begin the process of developing a superstructure and an infrastructure to deal with cybersecurity. We need more research. We need more scholars. We need more researchers, and we need more people who are capable of dealing directly with problems that occur.

We have heard mention of the electric grid and other such things as this; but it can appear in much more minor ways, simply denial of service which costs our economy billions of dollars each year. Recently, I had a call from someone who had received an e-mail sent by way of a government department's computer. A hacker had gotten into that computer and used this government's agency computer to send out millions of e-mails to prevent service from major entities in this country.

So I urge that we join together and we pass this bill and also be sure to alert the American public of the nature of cyberterrorism, cyberinsecurity and that we deal with this problem.

Mr. BAIRD. Mr. Chairman, I reserve my time.

The CHAIRMAN. Without objection, the gentlewoman from Maryland (Mrs. MORELLA) will control the majority's time.

There was no objection.

Mrs. MORELLA. Mr. Chairman, I am pleased to yield 2½ minutes to the gentleman from Illinois (Mr. WELLER).

Mr. WELLER. Mr. Chairman, I come to the floor and first want to commend the gentleman from New York (Mr. BOEHLERT) and the gentleman from Texas (Mr. HALL) for their bipartisan efforts to address an issue that is so very important to our Nation's economy and Nation's infrastructure.

We are at war today. We are at war against terrorism, and one of the lessons of September 11 is no more complacency. Clearly our Nation's IT infrastructure is one area where we historically have been very, very complacent; and as we work to win this war on terrorism, we also must work to strengthen our homeland security, and clearly this legislation, the Cyber Security Research and Development Act, is part of our efforts to strengthen our Nation's homeland security.

Our IT infrastructure is important. We use it in our everyday lives, whether it is our banking, insurance, our schools, our businesses, how we operate our utilities, and serve our Nation's infrastructure; and all of it is in jeopardy of a cyberattack.

All of us have learned, I believe, over the last several years the creativity of those who hack into our computer systems, those who create computer viruses for malicious destruction, in many cases causing billions of dollars of damage and costs to our Nation as well as our global economy. Unfortunately, very little research and development has been conducted in this important area of homeland security, finding better ways to protect our Nation's information technology systems.

The private sector historically has little incentive to invest because the market emphasizes speed and convenience. Yet the Federal Government historically has not filled the gap. This legislation is important legislation and deserves bipartisan support and enlists our Nation's universities as well as research institutions to find solutions to protect and secure our Nation's IT infrastructure.

There is also more we need to do. I think we are all disappointed after the House passed an economic stimulus package that the accelerated depreciation component that this House passed was not included in action in the other body. My hope is that the accelerated depreciation which would help our businesses and private sector also acquire the hardware and software to protect their IT systems will eventually be included in a stimulus package that we send to the President and get this economy moving again.

□ 1115

Mr. BOEHLERT. Mr. Chairman, I yield 4 minutes to the distinguished gentlewoman from Maryland (Mrs. MORELLA), who is one of the leaders of the Committee on Science in so many areas, but particularly interested in this important area.

Mrs. MORELLA. Mr. Chairman, it is with great pleasure that I rise as a cosponsor of H.R. 3394, and I thank the gentleman from New York (Mr. BOEHLERT) not only for his laudatory words but for his leadership as chairman of the Science Committee in crafting this piece of legislation and bringing it to the floor.

The ranking member, the gentleman from Texas (Mr. HALL), deserves to be commended also for working together. As is often the case with legislation from the Committee on Science, this bill is the outcome of a tremendous bipartisan effort, and I urge my colleagues to support its passage.

Computer networks and infrastructure have become one of America's greatest assets. Our ingenuity in developing new and exciting technologies to increase our productivity and quality of life have made us the envy of the modern world. These devices have changed the way we interact socially, conduct business, and have ingrained themselves in every aspect of our lives. We have embraced them and will continue to find exciting new ways to utilize these modern marvels.

Unfortunately, while these computer networks have given us great freedom and access, they have also created a new vulnerability. Our reliance on these networks creates a potential threat and the economic and social consequences to an attack in cyberspace cannot be ignored. In the past few months, we have been confronted with a number of threats to our physical well-being and have taken numerous steps to plug the many holes in our society's lax security practices. However, along with securing our borders and providing for defense of the homeland, we must also take steps to protect our virtual world.

As numerous hearings conducted in the House Committee on Science have shown, it is clear that we have two major problems in cyberspace. The first is that we have few, if any, standards as to what constitutes a secured network, nor do we have generally accepted procedures to evaluate our current systems and upgrade them with the most current security protocols. The second is quite simply too little cybersecurity research is being conducted by too few researchers and too few students to lead to the breakthrough of advancements that we will need to secure our networks in the 21st century.

To address our deficiencies in evaluation and implementation, last session the House of Representatives passed H.R. 1259, a bill I sponsored with the input of the gentleman from Washington (Mr. BAIRD) and others, to upgrade the Computer Security Act of 1987 and give the National Institute of Standards and Technology the authority to develop and promote computer security standards within the Federal Government. Located in my home district of Montgomery County, Maryland, NIST is our Nation's premier developer of standards and guidelines and is ideally suited to lead our efforts in the implementation of security practices throughout our cyberworld.

Today, we take up the second issue. H.R. 3394 would provide critical funds to investigators to conduct groundbreaking research, anticipate future needs, and respond to new vulnerabilities. It supplies money to develop multidisciplinary centers between academia, business interests,

and government laboratories to further collaborative efforts. And it creates fellowships and scholarships to assure that we are training a sufficient number of new scientists to replace our current workforce and meet our future needs.

H.R. 1259 and H.R. 3394 represent two sides of the same cybersecurity coin. Implementation of current technology without inquiries into the next generation of countermeasures and best practices is as useless as research and development without evaluation and use. Last session, the House overwhelmingly approved the first step toward protecting our virtual presence with the passage of 1259, and today I urge my colleagues to take the second. Research into cybersecurity is vital to the health of our Nation. This bill provides the necessary tools.

I look forward to its passage and to working with Chairman BOEHLERT and Ranking Member HALL in getting both H.R. 1259 and 3394 through the Senate and into law.

Mr. BOEHLERT. Mr. Chairman, I yield 2 minutes to the gentleman from Virginia (Mr. GOODLATTE), the distinguished chair of the House Republican High Technology Working Group, and the cochair of the Congressional Internet Caucus, and a real leader in all aspects of information technology.

Mr. GOODLATTE. Mr. Chairman, I thank the chairman for his kind words, but I especially thank him for his leadership on this issue. I also thank the gentleman from Texas (Mr. HALL), the ranking Democrat; the gentleman from Texas (Mr. SMITH), the chairman of the Subcommittee on Crime, on which I serve; and the other cosponsors of this legislation for their leadership in getting this done.

This is a serious problem in this country. We are vulnerable in many, many ways to cybercrime and cyberterrorism, and this legislation will help to cure that problem. We are not doing enough in the area of research in this area. We are most certainly not doing enough in the area of producing enough people to work in government and in the private sector to make sure that the computer infrastructure of this country is protected against hackers and criminals and terrorists. This legislation is going to provide more resources for those colleges and universities and other institutions that do this research and train the people.

In this area, I have a university in my district, James Madison University, which has been identified by the National Security Agency as an institution of excellence in doing research and, more importantly, education in this area. But when they sit down to write the curriculum on how to prevent cybercrime, to teach people how to work for companies or the government in protecting the computer infrastructure, that curriculum does not even change on an annual basis, does not even change on a monthly basis. It changes on a weekly and daily basis as new information about viruses and other types of computer activity used by criminals and terrorists take place.

So I am strongly supportive of this legislation. I look forward to developing more curricula around the country to educate people and provide the literally tens of thousands of new jobs we are going to need in this country in this field, and this legislation lays the groundwork. I commend the gentleman from New York and others for bringing this legislation forward, and I strongly urge my colleagues to support it.

Mrs. MORELLA. Mr. Chairman, I thank the gentleman from Virginia for his comments, and I yield 4 minutes to the gentleman from Texas (Mr. SMITH), Chair of the Subcommittee on Crime, who helped to author this bill.

Mr. SMITH of Texas. Mr. Chairman, I thank the gentlewoman from Maryland and my colleague for yielding me this time.

Mr. Chairman, I support this legislation that increases the cybersecurity networks at our universities, businesses, and national laboratories. The facts speak for themselves. Last month, the CERT Coordination Center operated by Carnegie Mellon University reported that breaches in security of computer systems more than doubled from the year 2000 to 2001: 52,000 incidents were reported in 2001, up from 22,000 the year before. By comparison, in 1995, the number of incidents reported was only 2,400.

Last spring, the Subcommittee on Crime, of the Committee on the Judiciary, that I chair, held a series of hearings on cybercrime. We heard testimony from local, State, and Federal officials, as well as individuals from the private sector. A common theme emerged: the demand for highly-trained and skilled personnel to investigate computer crimes is tremendous. This problem is compounded by the rapid advances in technology which make continual training an absolute necessity.

In this new age we must have training both for a new generation of cyberwarriors, whose most important weapon is not a gun but a laptop, and for private sector companies who must continually protect their Internet presence. This bill seeks to expand what many States and cities are already doing: investing in cybersecurity training initiatives.

Mr. Chairman, in my hometown, the University of Texas at San Antonio has established the Center for Information Assurance and Security, CIAS. The CIAS will be the hub of a city initiative to research, develop, and address computer protection mechanisms to prevent and detect intrusions of computer networks.

This collaborative effort of CIAS brings together the best and brightest from the public sector, such as the Air Force Information Warfare Center, Air Intelligence Agency, and the FBI. The private sector, with such cybersecurity companies as Ball Aerospace, Digital Defense, SecureLogix, SecureInfo, and Symantec, also are contributing to this effort.

With funding provided in this bill, UTSA and dozens of other universities will be able to train the next generation of cyberwarriors, cyberdefenders, and what we call ''white hat netizens.'' This legislation supports the work at UTSA and other universities for students who want to pursue computer security studies.

While the benefits of the digital age are obvious, the Internet also has fostered an environment where hackers retrieve private data for amusement, individuals distribute software illegally, and viruses circulate with the sole purpose of debilitating computers. Mr. Chairman, a well-trained and highly skilled force of cyberprotectors is urgently needed, and I hope my colleagues will support this bill.

Mr. BOEHLERT. Mr. Chairman, I yield myself such time as I may consume.

Mr. Chairman, as we wrap up this debate, I know a lot of people are wondering what is the big deal about cybersecurity; and my own wife, Marianne, who is frequently at the computer when I am home, says that we have to do a better job of explaining the importance of this, and she is absolutely right.

So much of what we do in this Nation is dependent upon the security of our computer systems. Everything is dependent upon computer technology today: our financial networks, our communication systems, our electric power grid, our water supply. The list goes on and on. If we have a clever 15-year-old hacker penetrate that system, that is mischief. But when we have a terrorist with a potential to penetrate that system and misuse it, that is serious business.

What we are about is very serious business: to train skilled people and to place the emphasis that needs to be placed on protecting our cybersystem in every way, shape, or manner. That is why I am so pleased that the administration has worked so well with us; that this Committee on Science has done what it does traditionally on a bipartisan basis, with people like the gentleman from Washington (Mr. BAIRD), the gentleman from Texas (Mr. HALL), and the gentlewoman from Texas (Ms. EDDIE BERNICE JOHNSON) working with our side.

We are all in this together. We want to produce a product that is best for this Congress and best for America; and we have done so, and I am proud to be identified with it.

Mr. Chairman, I have no further requests for time, and I yield back the balance of my time.

Mr. BAIRD. Mr. Chairman, I yield myself such time as I may consume.

Mr. Chairman, I would just like to close as well by reiterating my thanks to Chairman BOEHLERT, Chairwoman MORELLA, Ranking Member HALL, as well as the committee staff.

Chairman BOEHLERT has stated it perfectly well: the American public often takes for granted our information infrastructure; but a coordinated attack on, for example, air traffic control, electrical power systems, or other major vital links in our information infrastructure, particularly if timed with a more conventional or even a more unconventional attack, could wreak havoc on our society and would clearly cost lives.

The importance of this bill cannot be overstated, and I commend the Chair and the ranking member for their leadership and appreciate the opportunity to work with them.

Mr. Chairman, I yield back the balance of my time.

The CHAIRMAN. All time for general debate has expired.

The bill shall be considered by sections as an original bill for the purpose of amendment, and pursuant to the rule, each section is considered read.

During consideration of the bill for amendment, the Chair may accord priority in recognition to a Member offering an amendment that he has printed in the designated place in the CONGRESSIONAL RECORD. Those amendments will be considered read.

The Clerk will designate section 1.

The text of section 1 is as follows:

H.R. 3394

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cyber Security Research and Development Act''.

SEC. 2. FINDINGS.

The Congress finds the following:

(1) Revolutionary advancements in computing and communications technology have interconnected government, commercial, scientific, and educational infrastructures—including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services—in a vast, interdependent physical and electronic network.

(2) Exponential increases in interconnectivity have facilitated enhanced communications, economic growth, and the delivery of services critical to the public welfare, but have also increased the consequences of temporary or prolonged failure.

(3) A Department of Defense Joint Task Force concluded after a 1997 United States information warfare exercise that the results ''clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure''.

(4) Computer security technology and systems implementation lack—

(A) sufficient long term research funding;

(B) adequate coordination across Federal and State government agencies and among government, academia, and industry;

(C) sufficient numbers of outstanding researchers in the field; and

(D) market incentives for the design of commercial and consumer security solutions.

(5) Accordingly, Federal investment in computer and network security research and development must be significantly increased to—

(A) improve vulnerability assessment and technological and systems solutions;

(B) expand and improve the pool of information security professionals, including researchers, in the United States workforce; and

(C) better coordinate information sharing and collaboration among industry, government, and academic research projects.

SEC. 3. DEFINITIONS.

For purposes of this Act—

(1) the term ''Director'' means the Director of the National Science Foundation; and

(2) the term ''institution of higher education'' has the meaning given that term in section 101 ofthe Higher Education Act of 1965 (20 U.S.C. 1001).

SEC. 4. NATIONAL SCIENCE FOUNDATION RESEARCH.

(a) COMPUTER AND NETWORK SECURITY RESEARCH GRANTS.—

(1) IN GENERAL.—The Director shall award grants for basic research on innovative approaches to the structure of computer and network hardware and software that are aimed at enhancing computer security. Research areas may include—

(A) authentication and cryptography;

(B) computer forensics and intrusion detection;

(C) reliability of computer and network applications, middleware, operating systems, and communications infrastructure; and

(D) privacy and confidentiality.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this section on a merit-reviewed competitive basis.

(3) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $35,000,000 for fiscal year 2003;

(B) $40,000,000 for fiscal year 2004;

(C) $46,000,000 for fiscal year 2005;

(D) $52,000,000 for fiscal year 2006; and

(E) $60,000,000 for fiscal year 2007.

(b) COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.—

(1) IN GENERAL.—The Director shall award multiyear grants, subject to the availability of appropriations, to institutions of higher education (or consortia thereof) to establish multidisciplinary Centers for Computer and Network Security Research. Institutions of higher education (or consortia thereof) receiving such grants may partner with one or more government laboratories or for-profit institutions.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) PURPOSE.—The purpose of the Centers shall be to generate innovative approaches to computer and network security by conducting cutting-edge, multidisciplinary research in computer and network security, including the research areas described in subsection (a)(1).

(4) APPLICATIONS.—An institution of higher education (or a consortium of such institutions) seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the research projects that will be undertaken by the Center and the contributions of each of the participating entities;

(B) how the Center will promote active collaboration among scientists and engineers from different disciplines, such as computer scientists, engineers, mathematicians, and social science researchers; and

(C) how the Center will contribute to increasing the number of computer and network security researchers and other professionals.

(5) CRITERIA.—In evaluating the applications submitted under paragraph (4), the Director shall consider, at a minimum—

(A) the ability of the applicant to generate innovative approaches to computer and network security and effectively carry out the research program;

(B) the experience of the applicant in conducting research on computer and network security and the capacity of the applicant to foster new multidisciplinary collaborations;

(C) the capacity of the applicant to attract and provide adequate support for undergraduate and graduate students and postdoctoral fellows to pursue computer and network security research; and

(D) the extent to which the applicant will partner with government laboratories or for-profit entities, and the role the government laboratories or for-profit entities will play in the research undertaken by the Center.

(6) ANNUAL MEETING.—The Director shall convene an annual meeting of the Centers in order to foster collaboration and communication between Center participants.

(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the National Science Foundation to carry out this subsection—

(A) $12,000,000 for fiscal year 2003;

(B) $24,000,000 for fiscal year 2004;

(C) $36,000,000 for fiscal year 2005;

(D) $36,000,000 for fiscal year 2006; and

(E) $36,000,000 for fiscal year 2007.

SEC. 5. NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY PROGRAMS.

(a) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education (or consortia thereof) to establish or improve undergraduate and master's degree programs in computer and network security, to increase the number of students who pursue undergraduate or master's degrees in fields related to computer and network security, and to provide students with experience in government or industry related to their computer and network security studies.

(2) MERIT REVIEW.—Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) USE OF FUNDS.—Grants awarded under this subsection shall be used for activities that enhance the ability of an institution of higher education (or consortium thereof) to provide high-quality undergraduate and master's degree programs in computer and network security and to recruit and retain increased numbers of students to such programs. Activities may include—

(A) revising curriculum to better prepare undergraduate and master's degree students for careers in computer and network security;

(B) establishing degree and certificate programs in computer and network security;

(C) creating opportunities for undergraduate students to participate in computer and network security research projects;

(D) acquiring equipment necessary for student instruction in computer and network security, including the installation of testbed networks for student use;

(E) providing opportunities for faculty to work with local or Federal Government agencies, private industry, or other academic institutions to develop new expertise or to formulate new research directions in computer and network security;

(F) establishing collaborations with other academic institutions or departments that seek to establish, expand, or enhance programs in computer and network security;

(G) establishing student internships in computer and network security at government agencies or in private industry;

(H) establishing or enhancing bridge programs in computer and network security between community colleges and universities; and

(I) any other activities the Director determines will accomplish the goals of this subsection.

(4) SELECTION PROCESS.—

(A) APPLICATION.—An institution of higher education (or a consortium thereof) seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum—

(i) a description of the applicant's computer and network security research and instructional capacity, and in the case of an application from a consortium of institutions of higher education, a description of the role that each member will play in implementing the proposal;

(ii) a comprehensive plan by which the institution or consortium will build instructional capacity in computer and information security;

(iii) a description of relevant collaborations with government agencies or private industry that inform the instructional program in computer and network security;

(iv) a survey of the applicant's historic student enrollment and placement data in fields related to computer and network security and a study of potential enrollment and placement for students enrolled in the proposed computer and network security program; and

(v) a plan to evaluate the success of the proposed computer and network security program, including post-graduation assessment of graduate school and job placement and retention rates as well as the relevance of the instructional program to graduate study and to the workplace.

(B) AWARDS.—(i) The Director shall ensure, to the extent practicable, that grants are awarded under this subsection in a wide range of geographic areas and categories of institutions of higher education.

(ii) The Director shall award grants under this subsection for a period not to exceed 5 years.

(5) ASSESSMENT REQUIRED.—The Director shall evaluate the program established under this subsection no later than 6 years after the establishment of the program. At a minimum, the Director shall evaluate the extent to which the grants achieved their objectives of increasing the quality and quantity of students pursuing undergraduate or master's degrees in computer and network security.

(6) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $15,000,000 for fiscal year 2003;

(B) $20,000,000 for fiscal year 2004;

(C) $20,000,000 for fiscal year 2005;

(D) $20,000,000 for fiscal year 2006; and

(E) $20,000,000 for fiscal year 2007.

(b) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT OF 1992.—

(1) GRANTS.—The Director shall provide grants under the Scientific and Advanced Technology Act of 1992 for the purposes of section 3(a) and (b) of that Act, except that the activities supported pursuant to this subsection shall be limited to improving education in fields related to computer and network security.

(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $1,000,000 for fiscal year 2003;

(B) $1,250,000 for fiscal year 2004;

(C) $1,250,000 for fiscal year 2005;

(D) $1,250,000 for fiscal year 2006; and

(E) $1,250,000 for fiscal year 2007.

(c) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs for graduate students who pursue computer and network security research leading to a doctorate degree by providing funding and other assistance, and by providing graduate students with research experience in government or industry related to the students' computer and network security studies.

(2) MERIT REVIEW.—Grants shall be provided under this subsection on a merit-reviewed competitive basis.

(3) USE OF FUNDS.—An institution of higher education shall use grant funds for the purposes of—

(A) providing fellowships to students who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are pursuing research in computer or network security leading to a doctorate degree;

(B) paying tuition and fees for students receiving fellowships under subparagraph (A);

(C) establishing scientific internship programs for students receiving fellowships under subparagraph (A) in computer and network security at for-profit institutions or government laboratories; and

(D) other costs associated with the administration of the program.

(4) FELLOWSHIP AMOUNT.—Fellowships provided under paragraph (3)(A) shall be in the amount of $25,000 per year, or the level of the National Science Foundation Graduate Research Fellowships, whichever is greater, for up to 3 years.

(5) SELECTION PROCESS.—An institution of higher education seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the instructional program and research opportunities in computer and network security available to graduate students at the applicant's institution; and

(B) the internship program to be established, including the opportunities that will be made available to students for internships at for-profit institutions and government laboratories.

(6) REVIEW OF APPLICATIONS.—In evaluating the applications submitted under paragraph (5), the Director shall consider—

(A) the ability of the applicant to effectively carry out the proposed program;

(B) the quality of the applicant's existing research and education programs;

(C) the likelihood that the program will recruit increased numbers of students to pursue and earn doctorate degrees in computer and network security;

(D) the nature and quality of the internship program established through collaborations with government laboratories and for-profit institutions;

(E) the integration of internship opportunities into graduate students' research; and

(F) the relevance of the proposed program to current and future computer and network security needs.

(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry our this subsection—

(A) $10,000,000 for fiscal year 2003;

(B) $20,000,000 for fiscal year 2004;

(C) $20,000,000 for fiscal year 2005;

(D) $20,000,000 for fiscal year 2006; and

(E) $20,000,000 for fiscal year 2007.

(d) GRADUATE RESEARCH FELLOWSHIPS PROGRAM SUPPORT.—Computer and network security shall be included among the fields of specialization supported by the National Science Foundation's Graduate Research Fellowships program under section 10 of the National Science Foundation Act of 1950 (42 U.S.C. 1869).

SEC. 6. CONSULTATION.

In carrying out sections 4 and 5, the Director shall consult with other Federal agencies.

SEC. 7. FOSTERING RESEARCH AND EDUCATION IN COMPUTER AND NETWORK SECURITY.

Section 3(a) of the National Science Foundation Act of 1950 (42 U.S.C. 1862(a)) is amended—

(1) by striking ''and'' at the end of paragraph (6);

(2) by striking the period at the end of paragraph (7) and inserting ''; and''; and

(3) by adding at the end the following new paragraph:

''(8) to take a leading role in fostering and supporting research and education activities to improve the security of networked information systems.''.

SEC. 8. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY RESEARCH PROGRAM.

The National Institute of Standards and Technology Act is amended—

(1) by moving section 22 to the end of the Act and redesignating it as section 32;

(2) by inserting after section 21 the following new section:

''RESEARCH PROGRAM ON SECURITY OF COMPUTER SYSTEMS

''SEC. 22. (a) ESTABLISHMENT.—The Director shall establish a program of assistance to institutions of higher education that enter into partnerships with for-profit entities to support research to improve the security of computer systems. The partnerships may also include government laboratories. The program shall—

''(1) include multidisciplinary, long-term, high-risk research;

''(2) include research directed toward addressing needs identified through the activities of the Computer System Security and Privacy Advisory Board under section 20(f); and

''(3) promote the development of a robust research community working at the leading edge of knowledge in subject areas relevant to the security of computer systems by providing support for graduate students, post-doctoral researchers, and senior researchers.

''(b) FELLOWSHIPS.—(1) The Director is authorized to establish a program to award post-doctoral research fellowships to individuals who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 4(a)(1) of the Cyber Security Research and Development Act.

''(2) The Director is authorized to establish a program to award senior research fellowships to individuals seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 4(a)(1) of the Cyber Security Research and Development Act. Senior research fellowships shall be made available for established researchers at institutions of higher education who seek to change research fields and pursue studies related to the security of computer systems.

''(3)(A) To be eligible for an award under this subsection, an individual shall submit

an application to the Director at such time, in such manner, and containing such information as the Director may require.

''(B) Under this subsection, the Director is authorized to provide stipends for post-doctoral research fellowships at the level of the Institute's Post Doctoral Research Fellowship Program and senior research fellowships at levels consistent with support for a faculty member in a sabbatical position.

''(c) AWARDS; APPLICATIONS.—The Director is authorized to award grants or cooperative agreements to institutions of higher education to carry out the program established under subsection (a). To be eligible for an award under this section, an institution of higher education shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

''(1) the number of graduate students anticipated to participate in the research project and the level of support to be provided to each;

''(2) the number of post-doctoral research positions included under the research project and the level of support to be provided to each;

''(3) the number of individuals, if any, intending to change research fields and pursue studies related to the security of computer systems to be included under the research project and the level of support to be provided to each; and

''(4) how the for-profit entities and any other partners will participate in developing and carrying out the research and education agenda of the partnership.

''(d) PROGRAM OPERATION.—(1) The program established under subsection (a) shall be managed by individuals who shall have both expertise in research related to the security of computer systems and knowledge of the vulnerabilities of existing computer systems. The Director shall designate such individuals as program managers.

''(2) Program managers designated under paragraph (1) may be new or existing employees of the Institute or individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970.

''(3) Program managers designated under paragraph (1) shall be responsible for—

''(A) establishing and publicizing the broad research goals for the program;

''(B) soliciting applications for specific research projects to address the goals developed under subparagraph (A);

''(C) selecting research projects for support under the program from among applications submitted to the Institute, following consideration of—

''(i) the novelty and scientific and technical merit of the proposed projects;

''(ii) the demonstrated capabilities of the individual or individuals submitting the applications to successfully carry out the proposed research;

''(iii) the impact the proposed projects will have on increasing the number of computer security researchers;

''(iv) the nature of the participation by for-profit entities and the extent to which the proposed projects address the concerns of industry; and

''(v) other criteria determined by the Director, based on information specified for inclusion in applications under subsection (c); and

''(D) monitoring the progress of research projects supported under the program.

''(e) REVIEW OF PROGRAM.—(1) The Director shall periodically review the portfolio of research awards monitored by each program manager designated in accordance with subsection (d). In conducting those reviews, the Director shall seek the advice of the Computer System Security and Privacy Advisory Board, established under section 21, on the appropriateness of the research goals and on the quality and utility of research projects managed by program managers in accordance with subsection (d).

''(2) The Director shall also contract with the National Research Council for a comprehensive review of the program established under subsection (a) during the 5th year of the program. Such review shall include an assessment of the scientific quality of the research conducted, the relevance of the research results obtained to the goals of the program established under subsection (d)(3)(A), and the progress of the program in promoting the development of a substantial academic research community working at the leading edge of knowledge in the field. The Director shall submit to Congress a report on the results of the review under this paragraph no later than six years after the initiation of the program.

''(f) DEFINITIONS.—For purposes of this section—

''(1) the term 'computer system' has the meaning given that term in section 20(d)(1); and

''(2) the term 'institution of higher education' has the meaning given that term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).''; and

(3) in section 20(d)(1)(B)(i) (15 U.S.C. 278g–3(d)(1)(B)(i)), by inserting ''and computer networks'' after ''computers''.

SEC. 9. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS, AND INFORMATION.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by adding at the end the following new subsection:

''(f) There are authorized to be appropriated to the Secretary $1,060,000 for fiscal year 2003 and $1,090,000 for fiscal year 2004 to enable the Computer System Security and Privacy Advisory Board, established by section 21, to identify emerging issues, including research needs, related to computer security, privacy, and cryptography and, as appropriate, to convene public meetings on those subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects.''.

SEC. 10. INTRAMUTAL SECURITY RESEARCH.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is further amended—

(1) by redesignating subsection (d) as subsection (e); and

(2) by inserting after subsection (c) the following new subsection:

''(d) As part of the research activities conducted in accordance with subsection (b)(4), the Institute shall—

''(1) conduct a research program to address emerging technologies associated with assembling a networked computer system from components while ensuring it maintains desired security properties;

''(2) carry out research and support standards development activities associated with improving the security of real-time computing and communications systems for use in process control; and

''(3) carry out multidisciplinary, long-term, high-risk research on ways to improve the security of computer systems.''.

SEC. 11. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology—

(1) for activities under section 22 of the National Institute of Standards and Technology Act, as added by section 8 of this Act—

(A) $25,000,000 for fiscal year 2003;

(B) $40,000,000 for fiscal year 2004;

(C) $55,000,000 for fiscal year 2005;

(D) $70,000,000 for fiscal year 2006;

(E) $85,000,000 for fiscal year 2007; and

(F) such sums as may be necessary for fiscal years 2008 through 2012; and

(2) for activities under section 20(d) of the National Institute of Standards and Technology Act, as added by section 10 of this Act—

(A) $6,000,000 for fiscal year 2003;

(B) $6,200,000 for fiscal year 2004;

(C) $6,400,000 for fiscal year 2005;

(D) $6,600,000 for fiscal year 2006; and

(E) $6,800,000 for fiscal year 2007.

SEC. 12. NATIONAL ACADEMY OF SCIENCES STUDY ON COMPUTER AND NETWORK SECURITY IN CRITICAL INFRASTRUCTURES.

(a) STUDY.—Not later than 3 months after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology shall enter into an arrangement with the National Research Council of the National Academy of Sciences to conduct a study of the vulnerabilities of the Nation's network infrastructure and make recommendations for appropriate improvements. The National Research Council shall—

(1) review existing studies and associated data on the architectural, hardware, and software vulnerabilities and interdependencies in United States critical infrastructure networks;

(2) identify and assess gaps in technical capability for robust critical infrastructure network security, and make recommendations for research priorities and resource requirements; and

(3) review any and all other essential elements of computer and network security, including security of industrial process controls, to be determined in the conduct of the study.

(b) REPORT.—The Director of the National Institute of Standards and Technology shall transmit a report containing the results of the study and recommendations required by subsection (a) to the Congress not later than 21 months after the date of enactment of this Act.

(c) SECURITY.—The Director of the National Institute of Standards and Technology shall ensure that no information that is classified is included in any publicly released version of the report required by this section.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology for the purposes of carrying out this section, $700,000.

Mr. BOEHLERT (during the reading). Mr. Chairman, I ask unanimous consent that the remainder of the bill be printed in the RECORD and open to amendment at any point.

The CHAIRMAN. Is there objection to the request of the gentleman from New York?

There was no objection.

The CHAIRMAN. Are there any amendments to the bill?

If not, under the rule, the Committee rises.

Mr. FORBES. Mr. Chairman, I rise today in strong support of the Cyber Security Research and Development Act, which will help the United States reduce its vulnerability to cyberattacks by terrorists and common criminals alike.

Cyber attacks may not bring the large scale death and destruction of attacks by biological or chemical agents or other weapons of mass destruction, but they are just as real a threat

to the American people. They hold the power to disrupt our way of life, harm people's personal interests, and cause tremendous losses for businesses.

Computers have become increasingly ubiquitous. More than half of all American use the Internet, with more than 2 million people going online for the first time each month. Computer-based technology powers the way we bank, the way we shop, and the way we exchange information. And, this makes nearly every American vulnerable to cyber threats.

The Cyber Security Research and Development Act will reduce that vulnerability in two ways. First, it will improve our research efforts so that we can stop cyber terrorists before they strike. Too few of our most gifted minds are working on this area of research. The funding available in this bill will power partnerships between the government and academia to remedy this Second, H.R. 3394 will improve our education programs so that average Americans can spot threats and react quickly.

As a member of the Science Committee, I heard the testimony of research experts who indicated how great the threat is and how much could be achieved to defeat it if we dedicated ourselves to this goal. That is why I am pleased to be a cosponsor of this legislation, and I urge my colleagues to support it today.

Mr. RODRIGUEZ. Mr. Chairman, I rise today in support of H.R. 3394, the Cyber Security Research and Development Act. This bill would strengthen our nation's ability to protect the critical infrastructure that supplies our water, keeps the electricity on in our homes, and ensures that our law enforcement officials have communication capabilities at all times.

San Antonio has been a leader in developing the type of technology and educational programs made possible under this bill. A growing partnership of educational, private enterprise and military expertise make San Antonio ''Cyber City'' USA.

The University of Texas at San Antonio has developed the Center for Infrastructure Assurance and Security to educate and train world-class information technology professionals. With a faculty drawn from both the private sector and the Air Force, this outstanding program will produce skilled graduates ready to meet the growing shortage of information technology professionals in the federal government and private sector. It will also serve as a educational program for mid-level professionals to improve their information technology job skills needed for their current job, or help them retrain in the information technology field.

San Antonio is also the home of the Information Technology and Assurance Academy, an innovative educational center devoted to talented 11th and 12th graders interested in information technology. The Academy will give these young minds an introduction to future career opportunities in the information and technology field. In addition to developing their interest in information technology, this program seeks to instill a sense of civic responsibility that will serve them and the community in which they live.

San Antonio has 45 private companies that have developed state-of-the-art information assurance technology. These companies lead the field in developing intrusion detection technology and providing vulnerability assessments for both the private sector and the government.

The military also has a world-class computer monitoring facility in San Antonio. The Air Force's computer emergency response team, located at Lackland Air Force Base, leads the DoD in intrusion technology, and helps protect Air Force computer systems, 24 hours a day, 7 days a week, around the globe. This system helps ensure that the computer systems used by our Armed Forces to protect our nation are free from hackers, viruses and other forms of cyber terrorism.

This bill would provide the nation with needed resources to fight the war on cyber terrorism. Homeland security starts at the local level and this bill would allow communities throughout the United States to educate and train qualified information professionals in their community and encourage research that would give the government and private industry the tools to protect our nation's critical infrastructure.

Ms. HART. Mr. Chairman, I rise today in support of H.R. 3394, the Cyber Security Research and Development Act.

H.R. 3394, seeks to address the vulnerability of the computer systems and networks that have become part of all our daily lives. It is all to clear to us, that we must be proactive and defend these systems from simple hackers to coordinated terrorist attacks.

At hearings on cyber security last year in the Science Committee, we heard updates on research and development in that field. The news was sobering. The information we were provided was that too little research being conducted in this area, too few researchers were prepared to meet the needs of securing our systems, too few students going into fields relating to cyber security, and there was inadequate coordination between government, academia and industry. This must change and we have great resources in western Pennsylvania to help deliver these changes.

Carnegie Mellon University (CMU), just outside of my district, has been a leader in the field of cyber security. In 2001, the National Security Council named them as a ''Center of Excellence in Security Education.'' Also, the CERT Coordination Center, a government-funded computer emergency-response team at CMU, helps to track the risks and frequencies of cyber crimes. According to the Center, there were 52,658 security breaches and attacks last year, up 50 percent from the previous year. The Center also got reports of 2,437 computer vulnerabilities, more than double the figures from the previous year. While having success with students in the field of cyber security, they, too, have expressed that deficiencies exist for cyber security. This includes the lack of undergraduates and graduates who can provide the necessary research.

The ''Cyber Security Research and Development Act'' provides help for these areas by making grants available under National Science Foundation (NSF) for: research in innovative computer and network security; establishment of Centers for Computer and Network Security research in partnership with other universities; enabling universities to offer fellowships; and research in industry and other opportunities for doctoral degrees. H.R. 3394 also provides grants to the National Institute of Standards and Technology (NIST) for: support for high-risk, cutting edge research by academics working with industry; and for the establishment of a fellowship to increase its number of researchers in computer and network security.

This important legislation will provide us with the necessary investment in cyber security and needed support of existing resources, so that we are not with out the necessary experts to protect our critical computer infrastructure from terrorist attacks.

□ 1130

Accordingly, the Committee rose; and the Speaker pro tempore (Mr. PICKERING) having assumed the chair, Mr. SUNUNU, Chairman of the Committee of the Whole House on the State of the Union, reported that that Committee, having had under consideration the bill (H.R. 3394) to authorize funding for computer and network security research and development and research fellowship programs, and for other purposes, pursuant to House Resolution 343, he reported the bill back to the House.

The SPEAKER pro tempore. Under the rule, the previous question is ordered.

The question is on the engrossment and third reading of the bill.

The bill was ordered to be engrossed and read a third time, and was read the third time.

The SPEAKER pro tempore. The question is on the passage of the bill.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. BOEHLERT. Mr. Speaker, I object to the vote on the ground that a quorum is not present and make the point of order that a quorum is not present.

The SPEAKER pro tempore. Evidently a quorum is not present.

The Sergeant at Arms will notify absent Members.

Pursuant to clause 8 of rule XX, this 15-minute vote on passage of H.R. 3394 will be followed by a 5-minute vote, if ordered, on agreeing to the Speaker's approval of the Journal.

The vote was taken by electronic device, and there were—yeas 400, nays 12, not voting 23, as follows:

[Roll No. 13]

YEAS—400

Abercrombie	Bishop	Cardin
Ackerman	Blumenauer	Carson (IN)
Aderholt	Blunt	Carson (OK)
Allen	Boehlert	Castle
Andrews	Boehner	Chabot
Armey	Bonilla	Chambliss
Baca	Bonior	Clay
Bachus	Boozman	Clayton
Baird	Borski	Clement
Baker	Boswell	Clyburn
Baldacci	Boucher	Coble
Baldwin	Boyd	Combest
Ballenger	Brady (PA)	Condit
Barcia	Brady (TX)	Conyers
Barr	Brown (FL)	Cooksey
Barrett	Brown (OH)	Costello
Bartlett	Brown (SC)	Cox
Barton	Bryant	Coyne
Bass	Burr	Cramer
Becerra	Buyer	Crane
Bentsen	Callahan	Crenshaw
Bereuter	Calvert	Crowley
Berkley	Camp	Culberson
Berman	Cannon	Cummings
Berry	Cantor	Cunningham
Biggert	Capito	Davis (CA)
Bilirakis	Capps	Davis (FL)

Davis (IL)
Davis, Jo Ann
Davis, Tom
Deal
DeFazio
DeGette
Delahunt
DeLauro
DeLay
DeMint
Deutsch
Diaz-Balart
Dicks
Dingell
Doggett
Dooley
Doolittle
Doyle
Dreier
Dunn
Edwards
Ehlers
Ehrlich
Emerson
Engel
English
Eshoo
Etheridge
Evans
Everett
Farr
Fattah
Ferguson
Filner
Fletcher
Foley
Forbes
Ford
Fossella
Frank
Frost
Gallegly
Ganske
Gekas
Gephardt
Gibbons
Gilchrest
Gillmor
Gilman
Gonzalez
Goode
Goodlatte
Gordon
Goss
Graham
Granger
Graves
Green (TX)
Green (WI)
Greenwood
Grucci
Gutierrez
Gutknecht
Hall (TX)
Hansen
Harman
Hart
Hastings (FL)
Hastings (WA)
Hayes
Hayworth
Herger
Hill
Hilliard
Hinchey
Hinojosa
Hobson
Hoeffel
Hoekstra
Holden
Holt
Honda
Hooley
Horn
Hostettler
Houghton
Hoyer
Hulshof
Hunter
Hyde
Inslee
Isakson
Israel
Issa
Istook
Jackson (IL)
Jackson-Lee (TX)
Jenkins
John
Johnson (CT)
Johnson (IL)
Johnson, E. B.
Johnson, Sam
Jones (OH)
Kanjorski
Kaptur
Keller
Kelly
Kennedy (MN)
Kennedy (RI)
Kerns
Kildee
Kilpatrick
Kind (WI)
King (NY)
Kirk
Kleczka
Knollenberg
Kolbe
Kucinich
LaFalce
LaHood
Lampson
Langevin
Lantos
Largent
Larsen (WA)
Larson (CT)
Latham
LaTourette
Leach
Lee
Levin
Lewis (CA)
Lewis (GA)
Lewis (KY)
Linder
Lipinski
LoBiondo
Lofgren
Lowey
Lucas (KY)
Lucas (OK)
Lynch
Maloney (CT)
Maloney (NY)
Manzullo
Markey
Mascara
Matheson
Matsui
McCarthy (MO)
McCarthy (NY)
McCollum
McCrery
McGovern
McHugh
McInnis
McIntyre
McKeon
McKinney
McNulty
Meehan
Meek (FL)
Meeks (NY)
Menendez
Mica
Millender-McDonald
Miller, Dan
Miller, Gary
Miller, George
Miller, Jeff
Mink
Mollohan
Moore
Moran (KS)
Moran (VA)
Morella
Murtha
Myrick
Nadler
Napolitano
Neal
Nethercutt
Ney
Northup
Nussle
Oberstar
Olver
Ortiz
Osborne
Ose
Otter
Owens
Oxley
Pallone
Pascrell
Pastor
Payne
Pelosi
Pence
Peterson (MN)
Peterson (PA)
Petri
Phelps
Pickering
Platts
Pombo
Pomeroy
Portman
Price (NC)
Pryce (OH)
Putnam
Quinn
Radanovich
Rahall
Ramstad
Rangel
Regula
Rehberg
Reyes
Reynolds
Rivers
Rodriguez
Roemer
Rogers (KY)
Rogers (MI)
Rohrabacher
Ros-Lehtinen
Ross
Rothman
Roybal-Allard
Rush
Ryun (KS)
Sabo
Sanchez
Sanders
Sandlin
Sawyer
Saxton
Schakowsky
Schiff
Schrock
Scott
Sensenbrenner
Serrano
Sessions
Shadegg
Shays
Sherman
Sherwood
Shimkus
Shows
Shuster
Simmons
Simpson
Skeen
Skelton
Smith (MI)
Smith (NJ)
Smith (TX)
Smith (WA)
Snyder
Souder
Spratt
Stark
Stearns
Stenholm
Strickland
Stump
Stupak
Sununu
Sweeney
Tanner
Tauscher
Tauzin
Taylor (MS)
Taylor (NC)
Terry
Thomas
Thompson (CA)
Thompson (MS)
Thornberry
Thune
Thurman
Tiahrt
Tiberi
Tierney
Toomey
Towns
Turner
Udall (CO)
Udall (NM)
Upton
Velazquez
Visclosky
Vitter
Walden
Walsh
Wamp
Watkins (OK)
Watson (CA)
Watt (NC)
Watts (OK)
Waxman
Weiner
Weldon (FL)
Weldon (PA)
Weller
Wexler
Wicker
Wilson (NM)
Wilson (SC)
Wolf
Woolsey
Wu
Wynn
Young (AK)
Young (FL)

NAYS—12

Akin
Collins
Duncan
Flake
Hefley
Jones (NC)
Kingston
Norwood
Paul
Royce
Schaffer
Tancredo

NOT VOTING—23

Blagojevich
Bono
Burton
Capuano
Cubin
Frelinghuysen
Hall (OH)
Hastert
Hilleary
Jefferson
Luther
McDermott
Obey
Pitts
Riley
Roukema
Ryan (WI)
Shaw
Slaughter
Solis
Traficant
Waters
Whitfield

□ 1152

Messrs. AKIN, HEFLEY and NORWOOD changed their vote from ''yea'' to ''nay.''

So the bill was passed.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

Stated for:

Ms. SOLIS. Mr. Speaker, during rollcall vote No. 13 on February 7, 2002, the voting machine malfunctioned and did not record my vote. Had it registered my vote, I would have voted ''yea.''

THE JOURNAL

The SPEAKER pro tempore (Mr. PICKERING). Pursuant to clause 8 of rule XX, the pending business is the question of the Speaker's approval of the Journal.

The question is on agreeing to the Speaker's approval of the Journal of the last day's proceedings.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

RECORDED VOTE

Mr. KOLBE. Mr. Speaker, I demand a recorded vote.

A recorded vote was ordered.

The SPEAKER pro tempore. This is a 5-minute vote.

The vote was taken by electronic device, and there were—ayes 363, noes 33, answered ''present'' 1, not voting 38, as follows:

[Roll No. 14]

AYES—363

Abercrombie
Ackerman
Akin
Allen
Andrews
Armey
Baca
Bachus
Baker
Baldacci
Baldwin
Ballenger
Barcia
Barr
Barrett
Bartlett
Barton
Bass
Becerra
Bentsen
Bereuter
Berkley
Berman
Berry
Biggert
Bilirakis
Bishop
Blumenauer
Blunt
Boehlert
Boehner
Bonilla
Bonior
Boozman
Borski
Boswell
Boucher
Boyd
Brady (TX)
Brown (FL)
Brown (OH)
Brown (SC)
Bryant
Burr
Buyer
Callahan
Calvert
Camp
Cannon
Cantor
Capito
Capps
Cardin
Carson (IN)
Carson (OK)
Castle
Chabot
Chambliss
Clay
Clayton
Clement
Clyburn
Coble
Collins
Combest
Condit
Cooksey
Cox
Coyne
Cramer
Crenshaw
Crowley
Culberson
Cummings
Cunningham
Davis (CA)
Davis (FL)
Davis (IL)
Davis, Jo Ann
Davis, Tom
Deal
DeGette
Delahunt
DeLauro
DeLay
DeMint
Deutsch
Diaz-Balart
Dicks
Dingell
Doggett
Dooley
Doolittle
Doyle
Dreier
Duncan
Dunn
Edwards
Ehlers
Ehrlich
Emerson
Engel
Eshoo
Etheridge
Evans
Farr
Fattah
Ferguson
Flake
Fletcher
Foley
Forbes
Ford
Fossella
Frank
Frost
Ganske
Gekas
Gephardt
Gibbons
Gilchrest
Gillmor
Gilman
Gonzalez
Goode
Goodlatte
Gordon
Goss
Graham
Granger
Graves
Green (TX)
Green (WI)
Greenwood
Grucci
Hall (TX)
Hansen
Harman
Hart
Hastings (WA)
Hayes
Hayworth
Herger
Hill
Hilliard
Hinchey
Hinojosa
Hobson
Hoeffel
Holden
Holt
Honda
Hooley
Horn
Hostettler
Houghton
Hoyer
Hulshof
Hunter
Hyde
Inslee
Isakson
Israel
Issa
Istook
Jackson (IL)
Jackson-Lee (TX)
Jenkins
John
Johnson (CT)
Johnson (IL)
Johnson, Sam
Jones (NC)
Jones (OH)
Kanjorski
Kaptur
Keller
Kelly
Kennedy (RI)
Kerns
Kildee
Kilpatrick
Kind (WI)
King (NY)
Kirk
Kleczka
Knollenberg
Kolbe
Kucinich
LaFalce
LaHood
Lampson
Langevin
Lantos
Largent
Larson (CT)
LaTourette
Leach
Lee
Levin
Lewis (CA)
Lewis (GA)
Lewis (KY)
Lipinski
Lofgren
Lowey
Lucas (KY)
Lynch
Maloney (CT)
Maloney (NY)
Manzullo
Markey
Mascara
Matheson
Matsui
McCarthy (NY)
McCrery
McGovern
McHugh
McInnis
McIntyre
McKeon
McKinney
McNulty
Meehan
Meek (FL)
Meeks (NY)
Menendez
Mica
Millender-McDonald
Miller, Dan
Miller, Gary
Miller, Jeff
Mink
Mollohan
Moran (KS)
Moran (VA)
Morella
Murtha
Myrick
Nadler
Napolitano
Neal
Nethercutt
Ney
Northup
Norwood
Nussle
Olver
Ortiz
Osborne
Ose
Otter
Owens
Oxley
Pascrell
Pastor
Paul
Payne
Pelosi
Pence
Peterson (PA)
Petri
Phelps
Pickering
Platts
Pombo
Pomeroy
Portman
Price (NC)
Pryce (OH)
Putnam
Quinn
Radanovich
Rahall
Ramstad
Rangel
Regula
Rehberg
Reyes
Reynolds
Rivers
Rodriguez
Roemer
Rogers (KY)
Rogers (MI)
Rohrabacher
Ros-Lehtinen
Ross
Rothman
Roybal-Allard
Royce
Rush
Ryun (KS)
Sabo
Sanchez
Sanders
Sandlin
Sawyer
Saxton
Schiff
Schrock
Sensenbrenner
Serrano
Sessions
Shadegg
Shays
Sherman
Sherwood
Shimkus
Shows
Shuster
Simmons
Simpson
Skeen
Skelton
Smith (NJ)
Smith (TX)
Smith (WA)
Snyder
Solis
Souder
Spratt
Stearns
Stump
Stupak
Sununu
Sweeney
Tauscher
Tauzin
Thomas
Thornberry
Thune
Thurman
Tiahrt
Tiberi
Tierney
Toomey
Towns
Turner
Udall (CO)
Upton
Velazquez
Vitter
Walden
Walsh
Wamp
Watkins (OK)
Watson (CA)
Watt (NC)
Watts (OK)
Waxman
Weiner
Weldon (FL)
Weldon (PA)