By Mr. KERRY (for himself, Ms. SNOWE, Mr. LIEBERMAN, Mr. BENNETT, and Mr. BINGAMAN):

S. 1903. A bill to amend the Internal Revenue Code of 1986 to allow certain small businesses to defer payment of tax; to the Committee on Finance.

ADDITIONAL COSPONSORS

S. 1062

At the request of Mr. DURBIN, the name of the Senator from Michigan (Mr. LEVIN) was added as a cosponsor of S. 1062, a bill to amend the Public Health Service Act to promote organ donation and facilitate interstate linkage and 24-hour access to State donor registries, and for other purposes.

S. 1248

At the request of Mr. KERRY, the name of the Senator from New Jersey (Mr. TORRICELLI) was added as a cosponsor of S. 1248, a bill to establish a National Housing Trust Fund in the Treasury of the United States to provide for the development of decent, safe, and affordable, housing for low-income families, and for other purposes.

S. 1306

At the request of Mr. CRAIG, his name was added as a cosponsor of S. 1306, a bill to amend the Internal Revenue Code of 1986 to transfer all excise taxes imposed on alcohol fuels to the Highway Trust Fund, and for other purposes.

S. 1469

At the request of Mr. REED, the name of the Senator from New Jersey (Mr. CORZINE) was added as a cosponsor of S. 1469, a bill to amend the Head Start and Early Head Start programs to ensure that children eligible to participate in those programs are identified and treated for lead poisoning, and for other purposes.

S. 1566

At the request of Mr. REID, the name of the Senator from Washington (Ms. CANTWELL) was added as a cosponsor of S. 1566, a bill to amend the Internal Revenue code of 1986 to modify and expand the credit for electricity produced from renewable resources and waste products, and for other purposes.

S. 1607

At the request of Mr. ROCKEFELLER, the name of the Senator from North Dakota (Mr. CONRAD) was added as a cosponsor of S. 1607, a bill to amend title XVIII of the Social Security Act to provide coverage of remote monitoring services under the medicare program.

S. 1832

At the request of Mrs. LINCOLN, the name of the Senator from Massachusetts (Mr. KERRY) was added as a cosponsor of S. 1832, a bill to amend the Internal Revenue Code of 1986 to modify the credit for the production of electricity from renewable resources to include production of energy from agricultural and animal waste.

S. RES. 109

At the request of Mr. REID, the name of the Senator from Nebraska (Mr. HAGEL) was added as a cosponsor of S. Res. 109, a resolution designating the second Sunday in the month of December as ''National Children's Memorial Day'' and the last Friday in the month of April as ''Children's Memorial Flag Day''.

AMENDMENT NO. 2699

At the request of Mr. BUNNING, the name of the Senator from Oklahoma (Mr. INHOFE) was added as a cosponsor of amendment No. 2699.

AMENDMENT NO. 2717

At the request of Ms. COLLINS, the names of the Senator from Utah (Mr. BENNETT) and the Senator from Arkansas (Mr. HUTCHINSON) were added as cosponsors of amendment No. 2717 proposed to H.R. 622, a bill to amend the Internal Revenue Code of 1986 to expand the adoption credit, and for other purposes.

AMENDMENT NO. 2722

At the request of Mr. ALLARD, the name of the Senator from Virginia (Mr. WARNER) was added as a cosponsor of amendment No. 2722.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. EDWARDS:

S. 1900. A bill to protect against cyberterrorism and cybercrime, and for other purposes; the Committee on Commerce, Science, and Transportation.

By Mr. EDWARDS:

S. 1901. A bill to authorize the National Science Foundation and the National Security Agency to establish programs to increase the number of qualified faculty teaching advanced courses conducting research in the field of cybersecurity, and for other purposes; to the Committee on Health, Education, Labor, and Pensions.

Mr. EDWARDS. Mr. president, since the horrifying events of September 11, our country's number one priority has been to secure our families against the scourge of terrorism.

First, in our hearts, of course, are the men and women on the frontlines of the fight: the soldiers fighting for freedom half a world away; the firefighters and police officers in New York; the postal workers here in Washington.

Those of us elected to serve in Washington have a special responsibility to protect our security. To discharge that duty, I have been working with my colleagues here in the Senate. We have made a great deal of progress, but there's a lot more work to do.

After a long debate, Congress passed and the President signed important legislation, based partly on a bill I introduced, to tighten security in our airports. But we have to do more.

There are several bills that I have helped author that are working their way through Congress. Two of these bills, to tighten security at seaports and to protect against bioterrorism, have already passed the Senate and are awaiting action in the House. Another bill, to tighten our border security, should reach the Senate floor soon. All three should be enacted quickly. You can be sure our enemies are not waiting for us to act.

One of the greatest challenges in the struggle for security is to prepare for the next attack, not just the last one. We have seen how vicious thugs can destroy innocent life with airplanes, how they can terrorize ordinary people with biological weapons. We are responding to those threats. But what about threats whose awful consequences we haven't yet felt?

Today I want to talk about one of those threats: the threat of ''cyberterrorism'', an attack against the computer networks upon which our safety and economy now depend. Computers have become a foundation of our electricity, oil, gas, water, telephones, emergency services, and banks, not to mention our national defense apparatus.

Computer networks have brought extraordinary improvements in the way we live and work. We communicate more often, more quickly, more cheaply. With the push of a button in a classroom or a bedroom, our children can get more information than most libraries have ever held.

Yet there is a dark side to the internet, a new set of dangers. Today, if you ask an expert quietly, he or she will tell you that cyberspace is a very vulnerable place. Terrorists could cause terrible harm. They might be able to stop all traffic on the internet. Shut down power for entire cities for extended periods. Disrupt our phones. Poison our water. Paralyze our emergency services—police, firefighters, ambulances. The list goes on. We now live in a world where a terrorist can do as much damage with a keyboard and a modem as with a gun or a bomb.

Already, one hacker has broken into a computer-controlled waste management system and caused millions of gallons of raw sewage to spill into parks, rivers, and private property. You probably haven't heard about this attack because it occurred in Australia. But imagine if terrorists launched calculated, coordinated attacks on America.

Our enemies are already targeting our networks. After September 11, a Pakistani group hacked into two government web services, including one at the Department of Defense, and declared a ''cyber jihad'' against the United States. Another series of attacks, known as ''Moonlight Maze,'' assaulted the Pentagon, Department of Energy, and NASA, and obtained vast quantities of technical defense research. To date, we can be thankful that these attacks have not been terribly sophisticated. But that could change soon. As the Defense Science Board recently stated, the U.S. will eventually be attached ''by a sophisticated adversary using an effective array of information warfare tools and

techniques. Two choices are available: adapt before the attack or afterward.''

In addition, cybercrime is already a billion-dollar drain on our economy, a drain growing larger each year. In 1955, one survey reported that losses from FBI-reported computer crime had already reached $2 billion. Last year, the ''ILOVEYOU'' virus alone caused $8.7 billion in damage worldwide, much of it here. Cyberattacks have shut down major web sites like Yahoo! and eBay, not to mention the FBI. According to a recent survey, 85 percent of large corporations and government agencies detected computer security breaches over the prior 12 months. Two thirds suffered financial losses as a result.

So the danger is clear, and the only question is how we address it. I think we need to address it in many ways. Today I want to focus on just two that are especially critical.

The first is to encourage computer users to take proven measures to protect themselves. In the industry, these proven measures are known as ''best practices''—steps like using customized passwords, not the ones that come with software, or promptly installing known ''patches'' to keep intruders out.

The National Academy of Sciences recently reported that cybersecurity today is far worse than what known best practices can provide. As a result, viruses have shut down tens of thousands of machines even after patches to block them were widely available. Because the password protections on some systems are so weak, intruders have taken the ''routers'' that control Internet traffic hostage. And the government is as guilty as anyone. According to the report card issued by a member of the House of Representatives, most government agencies rate between a ''D'' and an ''F'' on cybersecurity. Improving our security by implementing existing best practices is our first big task.

Our second challenge is to train more researchers, teachers, and workers to fight cyberthreats. Today the private sector engages in some short-term R&D on cybersecurity. But broader research and knowledge needs aren't being met. In addition, our workforce in cybersecurity is woefully inadequate, especially in academia. Each year, American universities award Ph.D.'s in computer science to about one thousand people each year. But less than one-half of one-percent specialize in cybersecurity, and fewer still go on to train others in the discipline. As Dr. Bill Chu, Chairman of the Software and Information Systems Department at the University of North Carolina at Charlotte and one of the country's leading experts on cybersecurity puts it: ''The weakest link . . . is the lack of qualified information security professionals. The majority of information technology professionals in this country have not been trained in the basics of information security. Information technology faculty in most universities do not have sufficient background to properly train students.''

As a whole, the challenge of cybersecurity is not unlike the challenge of a terrible disease like cancer. First, we have to encourage everyone to do what they can to reduce the risk of disease—don't smoke, eat right, exercise. That is what cybersecurity ''best practices'' like changing passwords are all about. Second, we have to make sure we have got top-notch scientists working to find new medicines to prevent and fight the disease. And that is why we need more cyber teachers and researchers.

To tackle these two challenges, I'm proud today to introduce two new bills that will support an intensive, $400 million cybersecurity effort over the next five years. The first bill is called the Cyberterrorism Preparedness Act of 2002.

That bill's first step is to establish a new, nonprofit, nongovernment, consortium of academic and private sector experts to lay out a clear set of ''best practices'' that protect against cyberattack. The White House Office of Science and Technology Policy, the Institute for Defense Analyses, and the President's Committee of Advisors on Science and Technology have all recommended a new, nonprofit cybersecurity consortium. Such a consortium can work closely with the private sector, unfettered by bureaucracy, in a way that all the country can see and learn from.

The goals of the consortium are simple: first, the establishment of ''best practices'' that are tailored to different computer systems and needs; second, the widest possible dissemination of those practices; and third, long-term, multi-disciplinary research on cybersecurity-research that isn't occurring now.

The second part of the Cyberterrorism Preparedness Act will implement ''best practices'' for government systems. The government has a duty to lead by example, something we aren't doing right now. And so, within 6 months after this Act passed, the National Institute of Standards and Technology would immediately begin the process of implementing best practices for government agencies, beginning with small-scale tests and concluding with government-wide adoption of the recommended best practices.

The last part of my bill will assess the issue of best practices for the private sector. While the bill doesn't impose new mandates beyond the government, it does require careful consideration of how to encourage the widest possible use of known best practices. There's a particular focus on entities that do business with the Federal Government as grantees or contractors. Government agencies should not be exposed to security vulnerabilities in the products supplied by these companies. And Federal dollars should not be flowing to firms that expose America to cyberterrorism. So the new consortium would be required to study whether and how government could condition grants and contracts on the adoption of cybersecurity best practices. The President is authorized to implement recommendations from that study.

The Cyberterrorism Preparedness Act will address the first goal of cybersecurity—making sure we're taking the steps we already know to improve our security. The second bill I am introducing today—the Cybersecurity Research and Education Act—focuses on our second task: ''training the trainers'' and increasing the number of researchers, teachers, and workers committed to cybersecurity.

First, the bill establishes a Cybersecurity Graduate Fellowship Program at the National Science Foundation. Individuals selected to participate in the program will receive a loan that covers the full tuition and fees as well as a living stipend for 4 years of doctoral study. Upon graduation, these loans will be forgiven at 20 percent per year for each year that the individual teaches at a college or university. After only 5 years of teaching, the entire loan will be paid off. That way, we can ensure that the money we invest in these promising young scientists will be used to train others interested in cybersecurity.

Second, my bill also establishes a competitive sabbatical for Distinguished Faculty in Cybersecurity. Under the program, a qualified faculty member will receive a stipend to spend a year working and researching at the Department of Defense, a university specializing in cybersecurity, or some other appropriate facility. Universities sending faculty on sabbatical will receive funding to hire a temporary replacement instructor. In addition, when the faculty member returns, the university will get a generous grant to enhance its cybersecurity infrastructure needs. For example, the university could purchase advanced computing equipment and hire graduate research assistants. Participants in this program will have a unique opportunity to engage in cutting-edge research with some of the best minds in the country. When they return to their schools, these faculty will be even better equipped to advance the state of cybersecurity education.

Third, this bill will create a Cybersecurity Awareness, Training, and Education Program at the National Security Agency. NSA has a strong history of supporting cybersecurity education, as exemplified through initiatives such as the Centers of Excellence program and the National Colloquium for Information Systems Security Education. The program I propose would build on NSA's expertise and would enable the agency to make grants to universities specializing in cybersecurity. The grants could be used for projects like teaching basic computer security to K–12 teachers, or for the development of a ''virtual university.'' Students who don't

have access to nearby course offerings would then be able to take cybersecurity classes online.

All of these programs are critical in our fight against cyberterrorism. A strong and vibrant academic community is essential for building the trained workforce of tomorrow. We must be committed to funding long-term research. And we must vigilantly maintain basic cybersecurity protections in government, while promoting them in the private sector.

When it comes to the threat of a sophisticated, coordinated cyberterrorist attack, the question most likely is not whether such an attack will come. The question is when. And so we must be prepared to fight against a ''cyberjihad,'' and we must be prepared to win.

I ask unanimous consent that the text of my two bills be printed in the RECORD.

There being no objection, the bills were ordered to be printed in the RECORD, as follows:

S. 1900

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 ''Cyberterrorism Preparedness Act of 2002''.

SEC. 2. GRANT FOR PROGRAM FOR PROTECTION OF INFORMATION INFRASTRUCTURE AGAINST DISRUPTION.

(a) IN GENERAL.—The National Institute of Standards and Technology shall, using amounts authorized to be appropriated by section 5, award a grant to a qualifying nongovernmental entity for purposes of a program to support the development of appropriate cybersecurity best practices, support long-term cybersecurity research and development, and perform functions relating to such activities. The purpose of the program shall be to provide protection for the information infrastructure of the United States against terrorist or other disruption or attack or other unwarranted intrusion.

(b) QUALIFYING NONGOVERNMENTAL ENTITY.—For purposes of this section, a qualifying nongovernmental entity is any entity that—

(1) is a nonprofit, nongovernmental consortium composed of at least three academic centers of expertise in cybersecurity and at least three private sector centers of expertise in cybersecurity;

(2) has a board of directors of at least 12 members who include senior administrators of academic centers of expertise in cybersecurity and senior managers of private sector centers of expertise in cybersecurity and of whom not more than one third are affiliated with the centers comprising the consortium;

(3) is operated by individuals from academia, the private sector, or both who have—

(A) a demonstrated expertise in cybersecurity; and

(B) the capacity to carry out the program required under subsection (g);

(4) has in place a set of rules to ensure that conflicts of interest involving officers, employees, and members of the board of directors of the entity do not undermine the activities of the entity;

(5) has developed a detailed plan for the program required under subsection (g); and

(6) meets any other requirements established by the National Institute of Standards and Technology for purposes of this Act.

(c) APPLICATION.—Any entity seeking a grant under this section shall submit to the National Institute of Standards and Technology an application therefor, in such form and containing such information as the National Institute for Standards and Technology shall require.

(d) SELECTION OF GRANTEE.—The entity awarded a grant under this section shall be selected after full and open competition among qualifying nongovernmental entities.

(e) DISPERSAL OF GRANT AMOUNT.—Amounts available for the grant under this section pursuant to the authorization of appropriations in section 5 shall be dispersed on a fiscal year basis over the five fiscal years beginning with fiscal year 2003.

(f) CONSULTATION.—In carrying out activities under this section, including selecting an entity for the award of a grant, dispersing grant amounts, and overseeing activities of the entity receiving the grant, the National Institute of Standards and Technology—

(1) shall consult with an existing interagency entity, or new interagency entity, consisting of the elements of the Federal Government having a substantial interest and expertise in cybersecurity and designated by the President for purposes of this Act; and

(2) may consult separately with any such element of the Federal Government.

(g) PROGRAM USING GRANT AMOUNT.—

(1) IN GENERAL.—The entity awarded a grant under this section shall carry out a national program for the purpose of protecting the information infrastructure of the United States against disruption. The program shall consist of—

(A) multi-disciplinary research and development to identify appropriate cybersecurity best practices, to measure the effectiveness of cybersecurity best practices that are put into use, and to identify sound means to achieve widespread use of appropriate cybersecurity best practices that have proven effective;

(B) multi-disciplinary, long-term, or high-risk research and development (including associated human resource development) to improve cybersecurity; and

(C) the activities required under paragraphs (3) and (4).

(2) CONDUCT OF RESEARCH AND DEVELOPMENT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), research and development under subparagraphs (A) and (B) of paragraph (1) shall be carried out using funds and other support provided by the grantee to entities selected by the grantee after full and open competition among entities determined by the grantee to be qualified to carry out such research and development.

(B) CONDUCT BY GRANTEE.—The grantee may carry out research and development referred to in subparagraph (A) in any fiscal year using not more than 15 percent of the amount dispersed to the grantee under this Act in such fiscal year by the National Institute of Standards and Technology.

(3) RECOMMENDATIONS ON CYBERSECURITY BEST PRACTICES.—

(A) RECOMMENDATIONS.—Not later than 18 months after the selection of the grantee under this section, the grantee shall prepare a report containing recommendations for appropriate cybersecurity best practices.

(B) UPDATES.—The grantee shall update the recommendations made under subparagraph (A) not less often than once every six months, and may update any portion of such recommendations more frequently if the grantee determines that circumstances so require.

(C) CONSIDERATIONS.—In making recommendations under subparagraph (A), and any update of such recommendations under subparagraph (B), the grantee shall—

(i) review the most current cybersecurity best practices identified by the National Institute of Standards and Technology under section 3(a); and

(ii) consult with—

(I) the entities carrying out research and development under paragraph (1)(A);

(II) entities employing cybersecurity best practices; and

(III) a wide range of academic, private sector, and public entities.

(D) DISSEMINATION.—The grantee shall submit the report under subparagraph (A), and any update of the report under paragraph (B), to the bodies and officials specified in paragraph (5), and shall widely disseminate the report, and any such update, among government (including State and local government), private, and academic entities.

(4) ACTIVITIES RELATING TO WIDESPREAD USE OF CYBERSECURITY BEST PRACTICES.—

(A) IN GENERAL.—Not later than two years after the selection of the grantee under this section, the grantee shall submit to the bodies and officials specified in paragraph (5) a report containing—

(i) an assessment of the advisability of requiring the contractors and grantees of the Federal Government to use appropriate cybersecurity best practices; and

(ii) recommendations for sound means to achieve widespread use of appropriate cybersecurity best practices that have proven effective.

(B) REPORT ELEMENTS.—The report under subparagraph (A) shall set forth—

(i) whether or not the requirement described in subparagraph (A)(i) is advisable, including whether the requirement would impose undue or inappropriate burdens, or other inefficiencies, on contractors and grantees of the Federal Government;

(ii) if the requirement is determined advisable—

(I) whether, and to what extent, the requirement should be subject to exceptions or limitations for particular contractors or grantees, including the types of contractors or grantees and the nature of the exceptions or limitations; and

(II) which cybersecurity best practices should be covered by the requirement and with what, if any, exceptions or limitations; and

(iii) any other matters that the grantee considers appropriate.

(5) SPECIFIED BODIES AND OFFICIALS.—The bodies and officials specified in this paragraph are as follows:

(A) The appropriate committees of Congress.

(B) The President.

(C) The Director of the Office of Management and Budget.

(D) The National Institute of Standards and Technology.

(E) The interagency entity designated by the President under subsection (f)(1).

(h) GRANT ADMINISTRATION.—

(1) USE OF GRANT COMPETITION AND MANAGEMENT SYSTEMS.—The National Institute of Standards and Technology may permit the entity awarded the grant under this section to utilize the grants competition system and grants management system of the National Institute of Standards and Technology for purposes of the efficient administration of activities by the entity under subsection (g).

(2) RULES.—The National Institute of Standards and Technology shall establish any rules and procedures that the National Institute of Standards and Technology considers appropriate to further the purposes of this section. Such rules may include provisions relating to the ownership of any intellectual property created by the entity

awarded the grant under this section or funded by the entity under subsection (g).

(i) SUPPLEMENT NOT SUPPLANT.—The National Institute of Standards and Technology shall take appropriate actions to ensure that activities under this section supplement, rather than supplant, other current governmental and nongovernmental efforts to protect the information infrastructure of the United States.

SEC. 3. APPROPRIATE CYBERSECURITY BEST PRACTICES FOR THE FEDERAL GOVERNMENT.

(a) NIST RECOMMENDATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the National Institute of Standards and Technology shall submit to the bodies and officials specified in subsection (e) a report that—

(A) identifies appropriate cybersecurity best practices that could reasonably be adopted by the departments and agencies of the Federal Government over the 24-month period beginning on the date of the report; and

(B) sets forth proposed demonstration projects for the adoption of such best practices by various departments and agencies of the Federal Government beginning 90 days after the date of the report.

(2) UPDATES.—The National Institute of Standards and Technology may submit to the bodies and officials specified in subsection (e) any updates of the report under paragraph (1) that the National Institute of Standards and Technology consider appropriate due to changes in circumstances.

(3) CONSULTATION.—In preparing the report under paragraph (1), and any updates of the report under paragraph (2), the National Institute of Standards and Technology shall consult with departments and agencies of the Federal Government having an interest in the report and such updates, and with academic centers of expertise in cybersecurity and private sector centers of expertise in cybersecurity.

(b) DEMONSTRATION PROJECTS FOR IMPLEMENTATION OF RECOMMENDATIONS.—

(1) IN GENERAL.—Commencing not later than 90 days after receipt of the report under subsection (a), the President shall carry out the demonstration projects set forth in the report, including any modification of any such demonstration project that the President considers appropriate.

(2) UPDATES.—If the National Institute of Standards and Technology updates under subsection (a)(2) any recommendation under subsection (a)(1)(A) that is relevant to a demonstration project under paragraph (1), the President shall modify the demonstration project to take into account such update.

(3) REPORT.—Not later than nine months after commencement of the demonstration projects under this subsection, the President shall submit to the appropriate committees of Congress a report on the demonstration projects. The report shall set forth the following:

(A) An assessment of the extent to which the adoption of appropriate cybersecurity best practices by departments and agencies of the Federal Government under the demonstration projects has improved cybersecurity at such departments and agencies.

(B) An assessment whether or not the adoption of appropriate cybersecurity best practices by departments and agencies of the Federal Government under the demonstration projects has affected the capability of such departments and agencies to carry out their missions.

(C) A description of the cost of the adoption of appropriate cybersecurity best practices by departments and agencies of the Federal Government under the demonstration projects.

(D) A description of a security-enhancing missions-comparable, cost-effective program, to the extent such program is feasible, for the adoption of appropriate cybersecurity best practices government-wide.

(E) Any other matters that the President considers appropriate.

(c) ADOPTION OF CYBERSECURITY BEST PRACTICES GOVERNMENT-WIDE.—The President shall implement a program for the adoption of appropriate cybersecurity best practices government-wide commencing not later than six months after the date of the report.

(d) INCORPORATION OF RECOMMENDATIONS.—If during the development or implementation of the program under subsection (c) the President receives any recommendations under paragraph (3) or (4) of section 3(g), the President shall modify the program in order to take into account such recommendations.

(e) SPECIFIED BODIES AND OFFICIALS.—The bodies and officials specified in this subsection are as follows:

(1) The appropriate committees of Congress.

(2) The President.

(3) The Director of the Office of Management and Budget.

(4) The interagency entity designated by the President under section 3(f)(1).

SEC. 4. DEFINITIONS.

In this Act:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committee on Commerce, Science, and Transportation of the Senate; and

(B) the Committee on Science of the House of Representatives.

(2) CYBERSECURITY.—The term ''cybersecurity'' means information assurance, including information security, information technology disaster recovery, and information privacy.

(3) CYBERSECURITY BEST PRACTICE.—The term ''cybersecurity best practice'' means a computer hardware or software configuration, information system design, operational procedure, or measure, structure, or method that most effectively protects computer hardware, software, networks, or network elements against an attack that would cause harm through the installation of unauthorized computer software, saturation of network traffic, alteration of data, disclosure of confidential information, or other means.

(4) APPROPRIATE CYBERSECURITY BEST PRACTICE.—The term ''appropriate cybersecurity best practice'' means a cybersecurity best practice that—

(A) permits, as needed, customization or expansion for the computer hardware, software, network, or network element to which the best practice applies;

(B) takes into account the need for security protection that balances—

(i) the risk and magnitude of harm threatened by potential attack; and

(ii) the cost of imposing security protection; and

(C) takes into account the rapidly changing nature of computer technology.

SEC. 5. AUTHORIZATION OF APPROPRIATIONS.

There is hereby authorized to be appropriated for the National Institute of Standards and Technology for purposes of activities under this Act, amounts as follows:

(1) For fiscal year 2003, $70,000,000.

(2) For each of the fiscal years 2004 through 2007, such sums as may be necessary.

S. 1901

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 ''Cybersecurity Research and Education Act of 2002''.

SEC. 2. FINDINGS.

Congress finds that—

(1) critical elements of the Nation's basic economic and physical infrastructure rely on information technology for effective functioning;

(2) increased reliance on technology has left our Nation vulnerable to the threat of cyberterrorism;

(3) long-term research on practices, methods, and technologies that will help ensure the safety of our information infrastructure remains woefully inadequate;

(4) there is a critical shortage of faculty at institutions of higher education who specialize in disciplines related to cybersecurity;

(5) a vigorous scholarly community in fields related to cybersecurity is necessary to help conduct research and disseminate knowledge about the practical application of the community's findings; and

(6) universities in the United States award the Ph.D. degree in computer sciences to approximately 1,000 individuals each year, but of those awarded this degree, less than 0.3 percent specialize in cybersecurity and still fewer become employed in faculty positions at institutions of higher education.

SEC. 3. DEFINITIONS.

In this Act:

(1) CYBERSECURITY.—The term ''cybersecurity'' means information assurance, including scientific, technical, management, or any other relevant disciplines required to ensure computer and network security, including, but not limited to, a discipline related to the following functions:

(A) Secure System and network administration and operations.

(B) Systems security engineering.

(C) Information assurance systems and product acquisition.

(D) Cryptography.

(E) Threat and vulnerability assessment, including risk management.

(F) Web security.

(G) Operations of computer emergency response teams.

(H) Cybersecurity training, education, and management.

(I) Computer forensics.

(J) Defensive information operations.

(2) CYBERSECURITY INFRASTRUCTURE.—The term ''cybersecurity infrastructure'' includes—

(A) equipment that is integral to research and education capabilities in cybersecurity, including, but not limited to—

(i) encryption devices;

(ii) network switches;

(iii) routers;

(iv) firewalls;

(v) wireless networking gear;

(vi) protocol analyzers;

(vii) file servers;

(viii) workstations;

(ix) biometric tools; and

(x) computers; and

(B) technology support staff (including graduate students) that is integral to research and education capabilities in cybersecurity.

(3) DIRECTOR.—The term ''Director'' means the Director of the National Science Foundation.

(4) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given the term in section 101(a)

of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

(5) OTHER RELEVANT DISCIPLINE.—The term ''other relevant discipline'' includes, but is not limited to, the following fields as the fields specifically relate to securing information infrastructures:

(A) Biometrics.

(B) Software engineering.

(C) Computer science and engineering.

(D) Law.

(E) Business management or administration.

(F) Psychology.

(G) Mathematics.

(H) Sociology.

(6) QUALIFIED INSTITUTION.—The term ''qualified institution'' means an institution of higher education that, at the time of submission of an application pursuant to any of the programs authorized by this Act—

(A) has offered, for not less than 3 years prior to the date the application is submitted under this Act, a minimum of 2 graduate courses in cybersecurity (not including short-term special seminars or 1-time classes offered by visitors);

(B) has not less than 3 faculty members who teach cybersecurity courses—

(i) each of whom has published not less than 1 refereed cybersecurity research article in a journal or through a conference during the 2-year period preceding the date of enactment of this Act;

(ii) at least 1 of whom is tenured; and

(iii) each of whom has demonstrated active engagement in the cybersecurity scholarly community during the 2-year period preceding the date of enactment of this Act, such as serving as an editor of a cybersecurity journal or participating on a program committee for a cybersecurity conference or workshop;

(C) has graduated not less than 1 Ph.D. scholar in cybersecurity during the 2-year period preceding the date of enactment of this Act; and

(D) has not less than 3 graduate students enrolled who are pursuing a Ph.D. in cybersecurity.

SEC. 4. CYBERSECURITY GRADUATE FELLOWSHIP PROGRAM.

(a) PURPOSE.—The purpose of this section is—

(1) to encourage individuals to pursue academic careers in cybersecurity upon the completion of doctoral degrees; and

(2) to stimulate advanced study and research, at the doctoral level, in complex, relevant, and important issues in cybersecurity.

(b) ESTABLISHMENT.—The Director is authorized to establish a Cybersecurity Fellowship Program (referred to in this section as the ''fellowship program'') to annually award 3 to 5-year graduate fellowships to individuals for studies and research at the doctoral level in cybersecurity.

(c) CYBERSECURITY FELLOWSHIP PROGRAM ADVISORY BOARD.—

(1) ESTABLISHMENT.—There is established a Cybersecurity Fellowship Program Advisory Board (referred to in this section as the ''Board'').

(2) MEMBERSHIP.—The Director shall appoint members of the Board who shall include—

(A) not fewer than 3 full-time faculty members—

(i) each of whom teaches at an institution of higher education; and

(ii) each of whom has a specialty in cybersecurity; and

(B) not fewer than 2 research scientists employed by a Federal agency with duties that include cybersecurity activities.

(3) TERMS.—Members of the Board shall be appointed for renewable 2-year terms.

(d) APPLICATION.—Each individual desiring to receive a graduate fellowship under this section shall submit an application to the Director at such time, in such manner, and containing such information as the Director, in consultation with the Board, shall require.

(e) AWARD.—The Director is authorized to award graduate fellowships under the fellowship program that shall—

(1) be made available to individuals, through a competitive selection process, for study at a qualified institution and in accordance with the procedures established in subsection (h);

(2) be in an amount that is sufficient to cover annual tuition and fees for doctoral study at a qualified institution for the duration of the graduate fellowship, and shall include, in addition, an annual living stipend of $20,000; and

(3) be for a duration of 3 to 5-years, the specific duration of each graduate fellowship to be determined by the Director in consultation with the Board on a case-by-case basis.

(f) REPAYMENT.—Each graduate fellowship shall—

(1) subject to paragraph (f)(2), be subject to full repayment upon completion of the doctoral degree according to a repayment schedule established and administered by the Director;

(2) be forgiven at the rate of 20 percent of the total amount of graduate fellowship assistance received under this section for each academic year that a recipient is employed as a full-time faculty member at an institution of higher education for a period not to exceed 5 years; and

(3) be monitored by the Director to ensure compliance with this section.

(g) ELIGIBILITY.—To be eligible to receive a graduate fellowship under this section, an individual shall—

(1) be a citizen of the United States;

(2) be matriculated or eligible to be matriculated for doctoral studies at a qualified institution; and

(3) demonstrate a commitment to a career in higher education.

(h) SELECTION.—

(1) IN GENERAL.—The Director, in consultation with the Board, shall select recipients for graduate fellowships.

(2) DUTIES.—The Director, in consultation with the Board, shall—

(A) establish criteria for a competitive selection process for recipients of graduate fellowships;

(B) establish and promulgate an application process for the fellowship program;

(C) receive applications for graduate fellowships;

(D) annually review applications and select recipients of graduate fellowships; and

(E) establish and administer a repayment schedule for recipients of graduate fellowships.

(3) CONSIDERATION.—In making selections for graduate fellowships, the Director, to the extent possible and in consultation with the Board, shall consider applicants whose interests are of an interdisciplinary nature, encompassing the social scientific as well as technical dimensions of cybersecurity.

(i) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $5,000,000 for each of fiscal years 2003 through 2005, and such sums as may be necessary for each succeeding fiscal year.

SEC. 5. SABBATICAL FOR DISTINGUISHED FACULTY IN CYBERSECURITY.

(a) ESTABLISHMENT.—The Director is authorized to award grants to institutions of higher education to enable faculty members who are teaching cybersecurity subjects to spend a sabbatical from teaching working at—

(1) the National Security Agency;

(2) the Department of Defense;

(3) the National Institute of Standards and Technology;

(4) a research laboratory supported by the Department of Energy; or

(5) a qualified institution.

(b) APPLICATION.—Each institution of higher education desiring to receive a grant under this section shall submit an application to the Director at such time, in such manner, and containing such information as the Director shall require.

(c) GRANT AWARDS.—

(1) IN GENERAL.—The Director shall award a grant under this section only if the National Science Foundation and the agency or institution where the faculty member will spend the sabbatical approve the sabbatical placement.

(2) NUMBER AND DURATION.—For each fiscal year, the Director shall award grants for not more than 25 sabbatical positions that will each be for a 1-year period.

(3) AMOUNT OF AWARD.—

(A) IN GENERAL.—Each institution of higher education that is awarded a grant under this section shall receive $250,000 for each faculty member who will spend a sabbatical pursuant to the grant.

(B) USE OF AWARD.—The Director shall award a grant under this section in 2 disbursements in the following manner:

(i) FIRST DISBURSEMENT.—The first disbursement shall be made upon selection of a grant recipient and shall consist of the following:

(I) $20,000 to provide a stipend for living expenses to each faculty member awarded a sabbatical under this section.

(II) An amount sufficient for the grant recipient to hire a qualified replacement for the faculty member awarded a sabbatical under this section for the term of the sabbatical, if such a replacement is possible.

(ii) SECOND DISBURSEMENT.—The second disbursement shall be made at the conclusion of the sabbatical, only if the faculty member completes the sabbatical in its entirety, and shall be used for the grant recipient's cybersecurity infrastructure needs, including—

(I) acquiring equipment or technology;

(II) hiring graduate students; or

(III) supporting any other activity that will enhance the grant recipient's course offerings and research in cybersecurity.

(d) ELIGIBILITY.—To be eligible to receive a grant under this section, an institution of higher education shall submit an application under subsection (b) that—

(1) identifies the faculty member to whom the institution of higher education will provide a sabbatical and ensures that the faculty member is a citizen of the United States;

(2) ensures that the faculty member to whom the institution of higher education will provide a sabbatical is tenured at that institution of higher education and meets general standards of excellence in research or teaching; and

(3) explains how the faculty member to whom the institution of higher education will provide a sabbatical will—

(A) integrate into the faculty member's course offerings knowledge related to cybersecurity that is gained during the sabbatical; and

(B) in conjunction with the institution of higher education, use the second disbursement of funds available under subsection (c)(3)(B)(ii).

(e) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $8,000,000 for each of fiscal years 2003 through 2005.

SEC. 6. ENHANCING CYBERSECURITY INFRASTRUCTURE.

(a) ESTABLISHMENT.—The Director is authorized to award grants to qualified institutions to fund activities that provide, enhance, and facilitate acquisition of cybersecurity infrastructure at qualified institutions.

(b) USE OF GRANT AWARD.—Each qualified institution that receives a grant under this section shall use the grant funds for needs specifically related to—

(1) cybersecurity education and research; and

(2) development efforts related to cybersecurity.

(c) MATCHING FUNDS.—Each qualified institution that receives a grant under this section shall contribute to the activities assisted under this section non-Federal matching funds equal to not less than 25 percent of the amount of the grant.

(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $10,000,000 for each of fiscal years 2003 through 2005.

SEC. 7. CYBERSECURITY AWARENESS, TRAINING, AND EDUCATION PROGRAM.

(a) PURPOSE.—The purpose of this section is to increase the quality of education and training in cybersecurity, thereby increasing the number of qualified students entering the field of cybersecurity to adequately address the Nation's increasing dependence on information technology and to defend the Nation's increasingly vulnerable information infrastructure.

(b) ESTABLISHMENT.—The Director of the National Security Agency is authorized to award grants, on a competitive basis, to qualified institutions to establish Cybersecurity Awareness, Training, and Education Programs (referred to in this section as ''information programs'').

(c) APPLICATION.—

(1) IN GENERAL.—Each qualified institution desiring to receive a grant under this section shall submit an application to the Director of the National Security Agency at such time, in such manner, and accompanied by such information as the Director of the National Security Agency shall require.

(2) PLANS.—Each application submitted pursuant to paragraph (1) shall include a plan for establishing and maintaining an information program under this section, including a description of—

(A) the design, structure, and scope of the proposed information program, including unique qualities that may distinguish the proposed information program from possible approaches of other qualified institutions;

(B) research being conducted in the disciplines encompassed by the plan;

(C) any integration of the information program with other federally funded programs related to cybersecurity education, such as the National Science Foundation Scholarship for Service Program, the Department of Defense Multidisciplinary Research Program of the University Research Initiative, and the Department of Defense Information Assurance Scholarship Program;

(D) necessary costs for information infrastructure to support the information program;

(E) how the qualified institution will protect the integrity and security of the information infrastructure and any student testing mechanisms; and

(F) other relevant information.

(3) COLLABORATION.—A qualified institution desiring to receive a grant under this section may propose collaboration with other qualified institutions.

(d) GRANT AWARDS.—Each qualified institution that receives a grant under this section shall use the grant funds to—

(1) establish or enhance a Center for Studies in Cybersecurity Awareness, Training, and Education that shall—

(A) establish a professionally produced, web-based collection of cybersecurity programs of instruction that have been approved for general public dissemination by the authors and owners of the programs;

(B) maintain a web-based directory of cybersecurity education and training related conferences and symposia;

(C) sponsor the development of specific instructional materials in cybersecurity and other relevant disciplines, including—

(i) intrusion detection;

(ii) overview of information assurance;

(iii) ethical use of computing systems;

(iv) network security;

(v) cryptography;

(vi) risk management;

(vii) malicious logic; and

(viii) system security engineering;

(D) sponsor cybersecurity education symposia;

(E) collaborate with the National Colloquium for Information Assurance Education;

(F) create a 'Virtual Academy' for sharing courseware and laboratory exercises in cybersecurity; and

(G) review and participate in integrating various cybersecurity education and training standards into unified curricula; and

(2) establish or enhance a Center for the Development of Faculty in Cybersecurity that shall—

(A) establish criteria for recognition and certification of cybersecurity trainers and educators;

(B) establish faculty training outreach to teachers in kindergarten through grade 12 and to faculty of part B institutions (as defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061));

(C) build, test, and evaluate laboratory exercises that represent use of model practices in cybersecurity for use in training and education programs; and

(D) establish an integrated program to include the programs described in this paragraph and paragraph (1).

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section—

(1) $1,500,000 for fiscal year 2003;

(2) $2,000,000 for fiscal year 2004;

(3) $3,000,000 for fiscal year 2005; and

(4) $4,500,000 for fiscal year 2006.

SEC. 8. CYBERSECURITY WORKFORCE AND FACILITIES STUDY.

(a) STUDY.—The Comptroller General shall conduct a study and collect data on the following:

(1) The cybersecurity workforce, including—

(A) the size and nature of the cybersecurity workforce by occupation category (including academic faculty at institutions of higher education), level of education and training, personnel demographics, and industry characteristics; and

(B) the role of foreign workers in the cybersecurity workforce.

(2) Academic cybersecurity research facilities, including—

(A) total academic research space available or utilized for research relating to cybersecurity;

(B) academic research space relating to cybersecurity that is in need of major repair or renovation;

(C) new or ongoing projects at institutions of higher education expected to produce new or renovated research space to be used for research relating to cybersecurity; and

(D) any research space needs related to cybersecurity and based on projections of growth in educational programs and research, including costs and initiatives required to meet such needs and possible consequences of failure to meet such needs.

(3) Other information that the Comptroller General determines appropriate.

(b) REPORT.—Not later than 6 months after the date of enactment of this Act, and biennially thereafter, the Comptroller General shall prepare and submit a report on the study conducted pursuant to subsection (a) to the—

(1) Committee on Health, Education, Labor and Pensions of the Senate; and

(2) Committee on Education and the Workforce of the House of Representatives.

By Mr. KERRY (for himself, Ms. SNOWE, Mr. LIEBERMAN, Mr. BENNETT, and Mr. BINGAMAN):

S. 1903. A bill to amend the Internal Revenue Code of 1986 to allow certain small businesses to defer payment of tax; to the Committee on Finance.

Mr. KERRY. Mr. President, each year, the United States economy generates 600,000 to 800,000 new businesses. While many of these businesses will succeed, some of them will fail. Whether they succeed or not, one fact is without question: the entrepreneurs building these small businesses lay the foundation for our Nation's productivity gains, employment growth, and economic progress. In fact, although specific estimates vary, economists generally agree that small, entrepreneurial companies generate the majority of the Nation's new jobs.

The legislation I am introducing today, the Business Retained Income During Growth and Expansion, (BRIDGE), Act, will help ensure that rapidly expanding, entrepreneurial businesses have access to the capital they need to continue creating jobs and stimulating the economy.

Most new business start small and stay small. A portion, however, evolve into fast-growth companies with the capacity to propel the economy forward. For these companies, access to financing presents a pivotal challenge. A typical small business may open its doors with a combination of personal savings, credit card borrowing, and family lending. Informal investors, family, friends, and work associates, contribute the vast majority of the $56 billion of estimated initial funding for new businesses. If a business is successful, it moves to the next stage of development. Unfortunately, emerging growth companies will often outstrip the capital financing available based solely on the personal credit or assets of the entrepreneur.

Capital funding gaps frequently prevail when a firm seeks financing in the range of $250,000 to $1 million, a period when the business is particularly vulnerable. Funding needs below $250,000 are often fulfilled by family, friends, credit cards, home mortgages, and home equity lines of credit. Beyond $250,000, businesses typically turn to so-called ''angel'' financiers; high-interest borrowing; and in limited cases, Small Business Investment Companies. Venture capital is usually not an option for these companies because initial venture investments generally

begin at approximately $3 million, which is far more than most early-stage growth companies need or warrant. When sales reach $10 million, the company is better able to attract external financing at a reasonable cost based on the business's underlying assets.

Congress should take steps to ease the credit crunch for small businesses climbing the economic ladder from small to medium-size enterprise. When the lack of available financing prevents a growing, successful firm from expanding into new markets, we miss an opportunity to create new jobs and unleash productive forces. The legislation I am introducing today with Senator OLYMPIA SNOWE will help bridge the gap in capital financing for emerging growth companies. A companion measures has been introduced in the House by Representatives JIM DEMINT and BRIAN BAIRD.

The BRIDGE Act would allow mid-sized, fast-growing businesses to temporarily defer a portion of their Federal income tax liability if the firm's sales for the year are at least 10 percent higher than the average sales of the prior two years. The two-year deferral would be limited to $250,000 of tax, which would be repayable with interest over a four-year period. The tax-deferred amount would be deposited in a separate trust account at a bank or other approved intermediary, and the firm could borrow against the deferred amount, as collateral, for business purposes. Upon sale or merger of the business, any remaining tax deferral would be payable at that time.

To be eligible, a small business would have to have annual gross receipts of $10,000,000 or less. Partnerships and S corporations would also be eligible to make the election to defer taxes. To allow adequate review of this new and innovative concept, the proposal would expire at the end of 2005.

The BRIDGE Act will free up new investment capital for fast-growing firms by allowing them to use a portion of their federal tax liability for self-financing. These firms experience heavy demands on their cash flow as they reinvest receipts, hire new employees, create additional marketing channels, and purchase new equipment. Tax liability directly trades off with reinvestment. The BRIDGE Act will help reduce cash flow pressures by allowing a limited tax deferral. As the firm prospers, it will repay its original tax obligation as well as additional taxes on its higher receipts.

One of the most interesting aspects of the proposal is that its long-term costs are negligible. According to the Joint Committee on Taxation, the legislation would generate a revenue loss of $22.9 billion during the first four years. However, as businesses repay deferred amounts, the revenue loss would reverse, and then some. During the following six years, the proposal would raise $24.1 billion. Thus, over the ten year budget window, the proposal would raise $1.1 billion.

The entrepreneurial spirit lies at the foundation of our economy's technological advances, creative innovations, and dynamic growth. We should take steps to ensure that rapidly growing companies have the resources needed to continue producing new jobs and opportunities. The BRIDGE Act will free entrepreneurial businesses from the shackles of unmet capital funding needs and empower them to expand into new markets. I urge my colleagues to support the legislation, and I ask unanimous consent that the text of the legislation be printed in the RECORD.

There being no objection, the bill was ordered to be printed in the RECORD, as follows:

S. 1903

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 ''Business Retained Income During Growth and Expansion Act of 2002'' or the ''BRIDGE Act of 2002''.

SEC. 2. DEFERRED PAYMENT OF TAX BY CERTAIN SMALL BUSINESSES.

(a) IN GENERAL.—Subchapter B of chapter 62 of the Internal Revenue Code of 1986 (relating to extensions of time for payment of tax) is amended by adding at the end the following new section:

''SEC. 6168. EXTENSION OF TIME FOR PAYMENT OF TAX FOR CERTAIN SMALL BUSINESSES.

''(a) IN GENERAL.—An eligible small business may elect to pay the tax imposed by chapter 1 in 4 equal installments.

''(b) LIMITATION.—The maximum amount of tax which may be paid in installments under this section for any taxable year shall not exceed whichever of the following is the least:

''(1) The tax imposed by chapter 1 for the taxable year.

''(2) The amount contributed by the taxpayer into a BRIDGE Account during such year.

''(3) The excess of $250,000 over the aggregate amount of tax for which an election under this section was made by the taxpayer (or any predecessor) for all prior taxable years.

''(c) ELIGIBLE SMALL BUSINESS.—For purposes of this section—

''(1) IN GENERAL.—The term 'eligible small business' means, with respect to any taxable year, any person if—

''(A) such person meets the active business requirements of section 1202(e) throughout such taxable year,

''(B) the taxpayer has gross receipts of $10,000,000 or less for the taxable year,

''(C) the gross receipts of the taxpayer for such taxable year are at least 10 percent greater than the average annual gross receipts of the taxpayer (or any predecessor) for the 2 prior taxable years, and

''(D) the taxpayer uses an accrual method of accounting.

''(2) CERTAIN RULES TO APPLY.—Rules similar to the rules of paragraphs (2) and (3) of section 448(c) shall apply for purposes of this subsection.

''(d) DATE FOR PAYMENT OF INSTALLMENTS; TIME FOR PAYMENT OF INTEREST.—

''(1) DATE FOR PAYMENT OF INSTALLMENTS.—

''(A) IN GENERAL.—If an election is made under this section for any taxable year, the first installment shall be paid on or before the due date for such installment and each succeeding installment shall be paid on or before the date which is 1 year after the date prescribed by this paragraph for payment of the preceding installment.

''(B) DUE DATE FOR FIRST INSTALLMENT.—The due date for the first installment for a taxable year shall be whichever of the following is the earliest:

''(i) The date selected by the taxpayer.

''(ii) The date which is 2 years after the date prescribed by section 6151(a) for payment of the tax for such taxable year.

''(2) TIME FOR PAYMENT OF INTEREST.—If the time for payment of any amount of tax has been extended under this section—

''(A) INTEREST FOR PERIOD BEFORE DUE DATE OF FIRST INSTALLMENT.—Interest payable under section 6601 on any unpaid portion of such amount attributable to the period before the due date for the first installment shall be paid annually.

''(B) INTEREST DURING INSTALLMENT PERIOD.—Interest payable under section 6601 on any unpaid portion of such amount attributable to any period after such period shall be paid at the same time as, and as a part of, each installment payment of the tax.

''(C) INTEREST IN THE CASE OF CERTAIN DEFICIENCIES.—In the case of a deficiency to which subsection (e)(3) applies for a taxable year which is assessed after the due date for the first installment for such year, interest attributable to the period before such due date, and interest assigned under subparagraph (B) to any installment the date for payment of which has arrived on or before the date of the assessment of the deficiency, shall be paid upon notice and demand from the Secretary.

''(e) SPECIAL RULES.—

''(1) APPLICATION OF LIMITATION TO PARTNERS AND S CORPORATION SHAREHOLDERS.—

''(A) IN GENERAL.—In applying this section to a partnership which is an eligible small business—

''(i) the election under subsection (a) shall be made by the partnership,

''(ii) the amount referred to in subsection (b)(1) shall be the sum of each partner's tax which is attributable to items of the partnership and assuming the highest marginal rate under section 1, and

''(iii) the partnership shall be treated as the taxpayer referred to in paragraphs (2) and (3) of subsection (b).

''(B) OVERALL LIMITATION ALSO APPLIED AT PARTNER LEVEL.—In the case of a partner in a partnership, the limitation under subsection (b)(3) shall be applied at the partnership and partner levels.

''(C) SIMILAR RULES FOR S CORPORATIONS.—Rules similar to the rules of subparagraphs (A) and (B) shall apply to shareholders in an S corporation.

''(2) ACCELERATION OF PAYMENT IN CERTAIN CASES.—

''(A) IN GENERAL.—If—

''(i) the taxpayer ceases to meet the requirement of subsection (c)(1)(A), or

''(ii) there is an ownership change with respect to the taxpayer,

then the extension of time for payment of tax provided in subsection (a) shall cease to apply, and the unpaid portion of the tax payable in installments shall be paid on or before the due date for filing the return of tax imposed by chapter 1 for the first taxable year following such cessation.

''(B) OWNERSHIP CHANGE.—For purposes of subparagraph, in the case of a corporation, the term 'ownership change' has the meaning given to such term by section 382. Rules similar to the rules applicable under the preceding sentence shall apply to a partnership.

''(3) PRORATION OF DEFICIENCY TO INSTALLMENTS.—Rules similar to the rules of section 6166(e) shall apply for purposes of this section.

''(f) BRIDGE ACCOUNT.—For purposes of this section—

''(1) IN GENERAL.—The term 'BRIDGE Account' means a trust created or organized in

the United States for the exclusive benefit of an eligible small business, but only if the written governing instrument creating the trust meets the following requirements:

''(A) No contribution will be accepted for any taxable year in excess of the amount allowed as a deferral under subsection (b) for such year.

''(B) The trustee is a bank (as defined in section 408(n)) or another person who demonstrates to the satisfaction of the Secretary that the manner in which such person will administer the trust will be consistent with the requirements of this section.

''(C) The assets of the trust consist entirely of cash or of obligations which have adequate stated interest (as defined in section 1274(c)(2)) and which pay such interest not less often than annually.

''(D) The assets of the trust will not be commingled with other property except in a common trust fund or common investment fund.

''(E) Amounts in the trust may be used only—

''(i) as security for a loan to the business or for repayment of such loan, or

''(ii) to pay the installments under this section.

''(2) ACCOUNT TAXED AS GRANTOR TRUST.—The grantor of a BRIDGE Account shall be treated for purposes of this title as the owner of such Account and shall be subject to tax thereon in accordance with subpart E of part I of subchapter J of this chapter (relating to grantors and others treated as substantial owners).

''(3) TIME WHEN PAYMENTS DEEMED MADE.—For purposes of this section, a taxpayer shall be deemed to have made a payment to a BRIDGE Account on the last day of a taxable year if such payment is made on account of such taxable year and is made within 3½ months after the close of such taxable year.

''(g) REPORTS.—The Secretary may require such reporting as the Secretary determines to be appropriate to carry out this section.

''(h) APPLICATION OF SECTION.—This section shall apply to taxes imposed for taxable years beginning after December 31, 2001, and before January 1, 2006.''.

(b) PRIORITY OF LENDER.—Subsection (b) of section 6323 of the Internal Revenue Code of 1986 (relating to protection for certain interests even though notice filed) is amended by adding at the end the following new paragraph:

''(11) LOANS SECURED BY BRIDGE ACCOUNTS.—With respect to a BRIDGE account (as defined in section 6168(f)) with any bank (as defined in section 408(n)), to the extent of any loan made by such bank without actual notice or knowledge of the existence of such lien, as against such bank, if such loan is secured by such account.''.

(c) CLERICAL AMENDMENT.—The table of sections for subchapter B of chapter 62 of the Internal Revenue Code of 1986 is amended by adding at the end the following new item:

''Sec. 6168. Extension of time for payment of tax for certain small businesses.''.

(d) EFFECTIVE DATE.—The amendments made by this section shall apply to taxable years beginning after December 31, 2001.

(e) STUDY BY GENERAL ACCOUNTING OFFICE.—

(1) STUDY.—In consultation with the Secretary of the Treasury, the Comptroller General of the United States shall undertake a study to evaluate the applicability (including administrative aspects) and impact of the BRIDGE Act of 2001, including how it affects the capital funding needs of businesses under the Act and number of businesses benefiting.

(2) REPORT.—Not later than March 31, 2005, the Comptroller General shall transmit to the Committee on Ways and Means of the House of Representatives and the Committee on Finance of the Senate a written report presenting the results of the study conducted pursuant to this subsection, together with such recommendations for legislative or administrative changes as the Comptroller General determines are appropriate.

AMENDMENTS SUBMITTED AND PROPOSED

SA 2723. Mr. DOMENICI proposed an amendment to the language proposed to be stricken by amendment SA 2698 submitted by Mr. DASCHLE and intended to be proposed to the bill (H.R. 622) to amend the Internal Revenue Code of 1986 to expand the adoption credit, and for other purposes.

SA 2724. Mr. HATCH (for himself and Mr. BENNETT) proposed an amendment to the language proposed to be stricken by amendment SA 2698 submitted by Mr. DASCHLE and intended to be proposed to the bill (H.R. 622) supra.

SA 2725. Mr. BINGAMAN submitted an amendment intended to be proposed to the language proposed to be stricken by amendment SA 2698 submitted by Mr. DASCHLE and intended to be proposed to the bill (H.R. 622) supra; which was ordered to lie on the table.

SA 2726. Mrs. LINCOLN submitted an amendment intended to be proposed by her to the bill H.R. 622, supra; which was ordered to lie on the table.

SA 2727. Mr. ROCKEFELLER (for himself and Mr. KERRY, Mr. JOHNSON, and Mr. DASCHLE) submitted an amendment intended to be proposed by him to the bill H.R. 622, supra; which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 2723. Mr. DOMENICI proposed an amendment to the language proposed to be stricken by amendment SA 2698 submitted by Mr. DASCHLE and intended to be proposed to the bill (H.R. 622) to amend the Internal Revenue Code of 1986 to expand the adoption credit, and for other purposes; as follows:

At the end, add the following:

SEC. ___. PAYROLL TAX HOLIDAY.

(a) IN GENERAL.—Notwithstanding any other provision of law, the rate of tax with respect to remuneration received during the payroll tax holiday period shall be zero under sections 1401(a), 3101(a), and 3111(a) of the Internal Revenue Code of 1986 and for purposes of determining the applicable percentage under section 3201(a), 3211(a)(1), and 3221(a) of such Code.

(b) PAYROLL TAX HOLIDAY PERIOD.—The term ''payroll tax holiday period'' means the period beginning after February 28, 2002, and ending before April 1, 2002.

(c) EMPLOYER NOTIFICATION.—The Secretary of the Treasury shall notify employers of the payroll tax holiday period in any manner the Secretary deems appropriate.

(d) TRANSFER OF FUNDS.—The Secretary of the Treasury shall transfer from the general revenues of the Federal Government an amount sufficient so as to ensure that the income and balances of the trust funds under section 201 of the Social Security Act and the Social Security Equivalent Benefit Account under section 15A of the Railroad Retirement Act of 1974 (45 U.S.C. 231n–1) are not reduced as a result of the application of subsection (a).

(e) DETERMINATION OF BENEFITS.—In making any determination of benefits under title II of the Social Security Act, the Commissioner of Social Security shall disregard the effect of the payroll tax holiday period on any individual's earnings record.

SA 2724. Mr. HATCH (for himself and Mr. BENNETT!) PROPOSED AN AMENDMENT TO THE LANGUAGE PROPOSED TO BE STRICKEN BY AMENDMENT SA 2698 SUBMITTED BY MR. DASCHLE and intended to be proposed to the bill (H.R. 622) to amend the Internal Revenue Code of 1986 to expand the adoption credit, and for other purposes; as follows:

At the end, add the following:

SEC. ___. CARRYBACK OF CERTAIN NET OPERATING LOSSES ALLOWED FOR 7 YEARS.

(a) IN GENERAL.—Paragraph (1) of section 172(b) of the Internal Revenue Code of 1986 (relating to years to which loss may be carried) is amended by adding at the end the following new subparagraph:

''(H) SPECIAL RULE FOR CERTAIN LOSSES.—

''(i) IN GENERAL.—In the case of a taxpayer which has a net operating loss for any taxable year ending during 2000, 2001, or 2002, subparagraph (A)(i) shall be applied by substituting '7' for '2' and subparagraph (F) shall not apply.

''(ii) PER YEAR LIMITATION.—For purposes of the 6th and 7th taxable years preceding the taxable year of such loss, the amount of net operating losses to which clause (i) may apply for any taxable year shall not exceed $50,000,000.''

(b) ELECTION TO DISREGARD 7-YEAR CARRYBACK.—Section 172 of the Internal Revenue Code of 1986 (relating to net operating loss deduction) is amended by redesignating subsection (j) as subsection (k) and by inserting after subsection (i) the following new subsection:

''(j) ELECTION TO DISREGARD 7-YEAR CARRYBACK FOR CERTAIN NET OPERATING LOSSES.—Any taxpayer entitled to a 7-year carryback under subsection (b)(1)(H) from any loss year may elect to have the carryback period with respect to such loss year determined without regard to subsection (b)(1)(H). Such election shall be made in such manner as may be prescribed by the Secretary and shall be made by the due date (including extensions of time) for filing the taxpayer's return for the taxable year of the net operating loss. Such election, once made for any taxable year, shall be irrevocable for such taxable year.''

(c) TEMPORARY SUSPENSION OF 90 PERCENT LIMIT ON CERTAIN NOL CARRYBACKS.—

(1) IN GENERAL.—Subparagraph (A) of section 56(d)(1) of the Internal Revenue Code of 1986 (relating to general rule defining alternative tax net operating loss deduction) is amended to read as follows:

''(A) the amount of such deduction shall not exceed the sum of—

''(i) the lesser of—

''(I) the amount of such deduction attributable to net operating losses (other than the deduction attributable to carrybacks described in clause (ii)(I)), or

''(II) 90 percent of alternative minimum taxable income determined without regard to such deduction, plus

''(ii) the lesser of—

''(I) the amount of such deduction attributable to carrybacks of net operating losses for taxable years ending during 2000, 2001, or 2002, or

''(II) alternative minimum taxable income determined without regard to such deduction reduced by the amount determined under clause (i), and''.

(2) EFFECTIVE DATE.—The amendment made by this subsection shall apply to taxable years beginning before January 1, 2003.