Calendar No. 862

98TH CONGRESS, 2d Session } SENATE { REPORT 98–438

SMALL BUSINESS COMPUTER SECURITY AND EDUCATION ACT OF 1984

MAY 10 (legislative day, APRIL 30), 1984.—Ordered to be printed

Mr. WEICKER, from the Committee on Small Business, submitted the following

REPORT

[To accompany H.R. 3075]

The Committee on Small Business, to which was referred an Act (H.R. 3075) to amend the Small Business Act to establish a Small Business Computer Crime and Security Task Force, and for other purposes, having considered the same, reports favorably thereon with an amendment in the nature of a substitute, and an amendment to the title, and recommends that the bill, as amended, do pass.

I. COMMITTEE CONSIDERATION

H.R. 3075, an Act to amend the Small Business Act to establish a Small Business Computer Crime and Security Task Force, to study the magnitude and impact of computer crime on small business and provide small businesses with information necessary to improve their management of computer technology and to evaluate their computer security, was introduced by Congressman Wyden on May 19, 1983. The bill, with amendments, was passed by the House of Representatives on October 24, 1983, and the next day received in the Senate and referred to this Committee.

On October 4, 1983, Senators Tsongas, Nunn, and Boschwitz introduced S. 1920, a companion bill to H.R. 3075, which was also referred to this Committee.

H.R. 3075, as passed by the House of Representatives, requires the Small Business Administration (SBA) to establish a task force with representation from the public and private sector. Membership would include:

An employee of the SBA;

An employee of the Institute for Computer Sciences and

31–010 O

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

Technology;

An employee of the Department of Justice;

An employee of the Department of Defense;

A representative of the computer hardware industry;

A representative of the computer software industry;

A representative of the interests of providers of insurance to small business;

A representative of the interests of the providers of computer security services to small business;

A representative of the interests of associations of small business concerns; and

Additional appropriate individuals appointed by the Administration.

The purposes of the task force are to:

Define the nature and scope of computer crimes committed against small business concerns;

Ascertain the effectiveness of state legislation, and available security equipment, in preventing computer crimes against small business concerns;

Develop, in cooperation with the National Bureau of Standards, guidelines to assist small business concerns in evaluating the security of computer systems; and

Make recommendations to the SBA Administrator with respect to activities of the Resource Center.

The task force would have 18 months to submit a detailed report with recommendations to Congress, and would be terminated 30 days thereafter. After receipt of the task force report, the SBA would be required to establish a resource center to provide small business concerns with information regarding computer crimes and computer security techniques.

On March 7, 1984, Senator Tsongas chaired a full Committee hearing. Among the issues raised at the hearing were computer crime and its prevention as it affects the small business community, and small business computer security and management issues. At the hearing, the Committee received testimony from Congressman Wyden and Weber, the House cosponsors of H.R. 3075; Mr. James Thomson, Associate Administrator for Management Assistance at the Small Business Administration; Mr. Stuart Katzke, Manager of Computer Security for the Commerce Department's Institute for Computer Sciences and Technology; a representative of the insurance industry who specializes in liability coverage for small business computer users, and several computer crime and security experts who provide consultation to small businesses.

All of the witnesses agreed that computer crime is a growing small business concern and that the Federal Government, in cooperation with the private sector, can help provide information to the small business community on the need, and effective ways to protect itself from unauthorized computer entry. There was general agreement among the witnesses that the Small Business Administration would be the agency best able to coordinate the collection of such computer security information and use its extensive existing network of regional and district offices, and management assistance programs, to disseminate that

information to the small business community. No other Federal agency has such a large number of offices nationwide which counsel small business on a continuing basis. Mr. James Thomson, representing the Small Business Administration, made it clear that a key to the successful implementation of a computer security and education program would depend on the ability of his agency to undertake the activities recommended in the bill in close cooperation with profitmaking organizations. Mr. Thomson stated:

> The field of computer security, as well as the entire computer field and other high technology subjects such as the new communications technologies are becoming, critically important to small business. Most of the expertise in these areas is employed by profitmaking businesses with whom we cannot presently cosponsor. We believe these firms will work with us in helping small business when the proposed legislative change is enacted. Our mandate is to counsel and train small business and make them aware of potential problems. Utilization of profitmaking entities will enable us to outreach with the private sector in a shorter period of time with dramatically reduced costs.

Although the establishment of a computer security and education program has substantial support, serious questions were raised by the witnesses at the hearing regarding the need for, and the functions of, a task force as proposed in the House passed, and Senate introduced, legislation. According to the testimony, the general area of computer crime and unauthorized access has been studied and researched by Federal and private specialists. All concur that the lack of computer security controls pose a serious threat for small and large business computer users. Information on the nature of the problems does not seem to be lacking. However, there was an acknowledgement that there is no reliable information on the precise magnitude of computer crime, although some expert testimony placed the actual loss through direct computer crime at at least $1 billion. Therefore, most witnesses agreed that the recommended 18-month study period provided in both proposals would delay unnecessarily implementation of an educational program for the small business community without a significant benefit gained by the delay.

Some questions were raised about the emphasis of the task force on studying the scope of computer crime as it affects small businesses rather than focusing on computer crime prevention. Other questions were raised concerning the potential cost of establishing such a task force and providing staff support so that it could carry out its study mandate. Despite these concerns expressed about the task force, there was full agreement among the witnesses that, regardless of when the Small Business Administration proceeded with a computer security and education program, there was a definite need to provide SBA with expert advice and assistance in the development of such a program, particularly from other agencies in the Federal government such as the Commerce Department's Institute for Computer Sciences and Technology and the Department of Defense, and from the insurance industry, computer hardware and software manufacturers, computer

security experts in the private sector, and representatives of the small business community.

On May 8, 1984, the Committee met in executive session and, with a quorum present, agreed to favorably report out H.R. 3075, with an amendment in the nature of a substitute, and an amendment to the title. Significant changes agreed to by the Committee include:

The Task Force on Computer Crime is replaced by a Small Business Computer Security and Education Advisory Council which will meet at least once a year. Membership from the public and the private sector is the same as the Task Force. The Council will advise the SBA on the effectiveness of State and Federal laws in deterring computer crime and the effectiveness of computer technology and management techniques available to small businesses for increasing their computer security. The Council will also recommend to the agency appropriate functions for the computer security and education program.

No study report is required to be submitted to Congress.

The SBA would establish a computer security and education program rather than a resource center.

The SBA would gain the authority to cooperate with profitmaking organizations to provide management assistance to small business. This authority was requested by the Administration and was incorporated from a bill introduced by Senator Weicker (S. 1203).

Finally, SBA would be required to develop materials to carry out the computer security and information program in conjunction with ICST.

The Committee amendment is as follows:

Strike all after the enacting clause and insert the following:

SHORT TITLE

SECTION 1. This Act may be cited as the "Small Business Computer Security and Education Act of 1984".

FINDING AND PURPOSES

SEC. 2. (a) The Congress hereby finds that—

(1) there is increased dependency on, and proliferation of, information technology (including computers, data networks, and other communication devices) in the small business community;

(2) such technology has permitted an increase in criminal activity against small business;

(3) small businesses in particular frequently lack the education and awareness of computer security techniques and technologies which would enable them to protect their computer systems from unauthorized access and the manipulation or destruction of their computer hardware, software, and stored data;

(4) profitmaking organizations have substantial expertise in computer technology, communications, and management assistance that is not otherwise available; and

(5) the use of this expertise in the Small Business Administration's training delivery system would improve substantially the quantity and quality of the agency's management assistance programs.

(b) The purposes of this Act are—

(1) to improve the management by small businesses of their information technology,

(2) to educate and encourage small businesses to protect such technology from intentional or unintentional manipulation or destruction; and

(3) to encourage cooperation with profitmaking and nonprofitmaking organizations in providing management assistance to small business.

COMPUTER SECURITY AND EDUCATION ADVISORY COUNCIL

SEC. 3. Section 4(b) of the Small Business Act (15 U.S.C. 633(b)) is amended by adding at the end thereof the following:

"(3)(A) The Administrator shall, not later than ninety days after the effective date of the Small Business Computer Security and Education Act of 1984, establish an advisory council to be known as the Small Business Computer Security and Education Advisory Council (hereinafter referred to as the 'advisory council').

"(B) The advisory council shall consist of the following members:

"(i) an official of the Small Business Administration, appointed by the Administrator;

"(ii) an official of the Institute for Computer Sciences and Technology of the Department of Commerce, appointed by the Secretary of Commerce;

"(iii) an official of the Department of Justice, appointed by the Attorney General, who is knowledgeable about issues of computer security and its prosecution;

"(iv) an official of the Department of Defense, appointed by the Secretary of Defense, who is knowledgeable about issues of computer security;

"(v) one individual, appointed by the Administrator, who is representative of the interests of the manufacturers of computer hardware to small business concerns;

"(vi) one individual, appointed by the Administrator, who is representative of the interests of the manufacturers of computer software to small business concerns;

"(vii) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer liability insurance to small business concerns;

"(viii) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer security equipment and services to small business concerns;

"(ix) one individual, appointed by the Administrator, who is representative of the interests of associations of small business concerns, other than small business concerns engaging in any of the activities described in clauses (v) through (viii); and

"(x) such additional qualified individuals from the private sector, appointed by the Administrator, as the Administrator determines to be appropriate.

"(C) It shall be the function of the advisory council to advise the Administration on—

"(i) the nature and scope of computer crimes committed against small business concerns;

"(ii) the effectiveness of Federal and State law in deterring computer-related criminal activity or prosecuting computer-related crimes;

"(iii) the effectiveness of computer technology and management techniques available to small business for increasing their computer security;

"(iv) the development of information and guidelines to be made available to the Administrator to assist small business concerns in evaluating the security of computer systems; and

"(v) such other appropriate functions of the small business computer security and education program.

"(D) The Administrator shall designate one of the non-Federal members of the advisory council as its chairperson. The advisory council shall meet at least annually and at such other times as requested by the Administrator. A majority of the members of the advisory council shall constitute a quorum. Vacancies on the council shall be filled in the same manner as the original appointment.

"(E) Each member of the advisory council shall serve without additional pay, allowances, or benefits by reason of such service. Each non-Federal member shall be reimbursed for actual expenses, including travel expenses, as authorized by section 5703 of title 5, United States Code.

"(F) Upon request of the chairperson of the advisory council, the Administrator may request directly from any Federal agency information necessary to enable the advisory council to carry out its functions under the Small Business Computer Security and Education Act of 1984. Upon the request of the Administrator, the head of such agency shall furnish to the Administrator such information, subject to the requirements of section 552 of title 5, United States Code.".

COMPUTER SECURITY AND EDUCATION PROGRAM

SEC. 4. Section 4(b) of the Small Business Act (15 U.S.C. 633(b)) is further amended by adding at the end thereof the following:

"(4)(A) The Administrator shall establish a small business computer security and education program to—

"(i) provide small business concerns information regarding—

"(I) utilization and management of computer technology;

"(II) computer crimes committed against small business concerns; and

"(III) security for computers owned or utilized by small business concerns;

"(ii) provide for periodic forums for small business concerns to improve their knowledge of the matters described in clause (i); and

"(iii) provide training opportunities to educate small business users on computer security techniques.

"(B) The Administrator, after consultation with the Director of the Institute of Computer Sciences and Technology within the Department of Commerce, shall develop information and materials to carry out the activities described in subparagraph (A) of this paragraph.".

PRIVATE SECTOR COOPERATION

SEC. 5. Section 8(b)(1)(A) of the Small Business Act is amended—

(1) by inserting "computer security," after "wage incentives,";

(2) by inserting ", with profitmaking concerns," after "associations, and institutions"; and

(3) by adding before the semicolon at the end thereof ": Provided, That the Administration shall take such actions as it determines to be necessary to ensure that the participation by a profitmaking concern does not constitute an endorsement by the Federal Government of the products or services of any such concern, and to avoid the undue promotion of the products or services of any such profitmaking concern, but the mere participation by such concern shall not, in itself, be considered a promotion or endorsement of its products or services".

COMPUTER CRIME DEFINITION

SEC. 6. Section 3 of the Small Business Act is amended by adding at the end thereof the following—

"(j) For purposes of this Act—

"(1) the term 'computer crime' means—

"(A) any crime committed against a small business concern by means of the use of a computer; and

"(B) any crime involving the illegal use of, or tampering with, a computer owned or utilized by a small business concern.".

EFFECTIVE DATES

SEC. 7. (a) This Act shall take effect on October 1, 1984.

(b) The amendments made to section 4(b)(3) of the Small Business Act by section 3 of this Act are repealed on October 1, 1987. Nothing in this section shall preclude the Administrator from continuing such committee under the authority of section 8(b)(3) of the Small Business Act and the Federal Advisory Committee Act.

Amend the title so as to read:

An Act to amend the Small Business Act to establish a small business computer security and education program, and for other purposes.

II. NEED FOR LEGISLATION

The use of computers by small businesses has increased dramatically in the last 5 years, particularly as the cost and size of computer systems have diminished. Testimony before the Committee indicated that computer usage by small businesses is expected to jump by almost 50 per cent in the 1 year between mid-1983 and mid-1984, with the majority of sales being made to companies with less than 20 employees.

The increased use and reliance on computer technology by the business community has also provided new opportunities for abuse of the new technology for criminal purposes. According to Sanford Sherizen, president of Data Security Systems, Inc., there are four new rules for business in the age of computer:

1. Computer security is no longer an optional decision but may be fundamental to the survival of a business;
2. The core issues of computer security can and must be understood by nontechnical managers;
3. The essence of computer security lies with management controls, reviews and policies developed with the active support and involvement of top management; and
4. There are a variety of management questions which can be raised with technical staffs in order to evaluate the adequacy of computer protections in business.

Although the need for increased computer security is an issue common to both small and large businesses, it is clear that small business must contend with the threat of computer crime under fundamentally different circumstances than their large business counterparts. As explained by Dr. Leslie Ball, professor of information systems at Babson College, during the Committee's March 7th hearing:

> The problem that a small business has is the lack of management time and expertise. Virtually every small businessman has more tasks than he can complete in most business days. Computer crime is a low priority item for the small business person, and they do not have the expertise in-house to deal with the problem. Another issue is cost. To develop fairly secure systems requires a lot of money be spent. Excess cash for this type of investment is often not available to small businesses. For small businesses every spare dollar must be invested to yield a positive return.

Small business computer users tend to use smaller systems which, by their nature, tend to have more limited security features. Furthermore, many small businesses have little direct control over the information system they are using. They lease communication lines to tie into larger mainframe computers located outside of the business premises, use computers owned by others on a time-sharing basis, and use packaged software purchased off the shelf.

Experts have concluded that small businesses are increasingly finding themselves at greater risk to lapses in their computer security procedures, and therefore are more susceptible to being the victim of computer crime. Since these same businesses have fewer capital resources, they are also less able to absorb losses than their large business counterparts.

During the past 5 years, a few insurance companies have begun to respond to this problem with new insurance packages designed specifically for businesses which utilize mini-computers. Unfortunately, even though these policies are available at a relatively low cost, an insurance spokesman told the Committee that the majority of mini-computers used by small businesses remain uninsured.

At the Federal level, the Institute of Computer Sciences and Technology (ICST), within the Department of Commerce, is the governmental entity whose principal activities include developing information on computer security and related matters for the Federal Government. However, ICST does not have a specific legislative mandate to serve small business directly. The absence of this mandate, coupled with the lack of sufficient funds and personnel within the ICST, makes it unreasonable to expect that the task of providing significant information to the small business community is being effectively carried out. Within the private sector, a number of professional associations have begun, for a fee, to provide workshops and seminars on computer security techniques to their members.

While the initiative shown by the ICST and these professional associations is very positive, it nevertheless remains that there is no effective outreach program in either the public or private sector through which information regarding computer security and computer crime can be transmitted to the unaffiliated small business person. Therefore, while experts in the public and private sector agree that information and technologies exist in abundance, the small business community remains largely uninformed and the available solutions to the problems go underutilized.

H.R. 3075, as amended by the Committee, will address the information and training needs of the small business computer user. It is an inexpensive commonsense response to the growing problem of computer crime against small business. It allows the Small Business Administration to make full use of expertise in other Federal agencies and the private sector to provide an expanded quality management assistance program to small business.

III. Explanation of the Committee Amendment

The Committee amendment addresses the concerns of the Small Business Administration and several of the computer security experts who testified at the Committee's March 7 hearing on the need to proceed immediately to provide state of the art information to small businesses on computer related crime and abuse, and management information and training on associated computer security controls.

Most of the recent debate regarding the need for specific Federal legislation regarding computer crime has focused on the adequacy of existing criminal law to cover the full range of crimes associated with computer systems. Some 20 states have already enacted computer related crime legislation. The focus of other pending Federal legislation and state laws is for the most part on increased punishment for the crimes after they have been committed rather than the issue of prevention.

H.R. 3075, as amended by the Committee, focuses on prevention. Many small businesses have yet to learn how to use computers effec-

tively, how to protect their information, and how to safeguard their computers from accidental or deliberate misuse. The establishment of a "Small Business Computer Security and Education Program" by the SBA will result in providing needed education, training and information on these issues to a rapidly expanding audience of small business computer users.

The stakes are high. According to FBI statistics, the average bank robbery is $10,000. The FBI estimates that the average computer crime is over $400,000. According to one expert on computer crime, only one of the estimated 200,000 computer crimes committed each year is likely to be prosecuted. Few companies want to admit they were victims of computer theft because it could devastate a firm's image. Few attorneys or investigators at the State or Federal level have the training or experience to handle computer crimes.

The Committee amendment, with its emphasis on dissemination of information and training, should be of critical assistance to small businesses that cannot afford to hire consultants to fashion their security measures to deter computer crimes directed against them.

A. COMPUTER SECURITY AND EDUCATION PROGRAM

The Committee amendment mandates the establishment of a "Small Business Computer Security and Education Program" by the Small Business Administration. The SBA has already begun a number of efforts to inform small business about computer security concerns, including the preparation of a publication entitled "Computer Security Considerations for Small Business Systems", the furnishing of the National Bureau of Standards computer security bibliography, the purchasing of copies of a computer security film to be shown at training sessions, and the updating of present agency publications on business computers with newly acquired information on computer security.

The Committee believes that since the mission of the SBA under the Small Business Act is to aid, counsel, assist, and protect the interests of small business, it is appropriate for the SBA to assume the responsibility for the dissemination of computer crime detection, prevention, and security information to small businesses.

The Committee would expect that the small business computer security and education program would benefit from the large network of voluntary and cooperative resources that have been developed to provide management assistance to small businesses. Administered at the local level, this program would reach out to small businesses by utilizing the SBA's regional and district office structure and appropriate private sector resources.

As a delivery mechanism for information on computer fraud and security, the SBA already has in place the following management assistance resources: Service Corps of Retired Executives and Active Corps of Executives, Small Business Development Centers, Small Business Institutes, Chambers of Commerce, and the American Association of Community and Junior Colleges. These resources, in addition to the regional and district SBA offices, could prove to be an effective starting point for communicating important information about the utilization and management of computer technology and the preven-

tion of computer crime to small businesses, rather than relying on a single resource center located in Washington, D.C., as proposed in the House bill.

The Committee anticipates that the SBA will disseminate information on the utilization and management of computer technology, computer crimes committed against small business concerns, and computer security, through a variety of approaches. By sponsoring training opportunities, workshops, seminars, and periodic forums, the SBA should be able to assist small business computer users.

The Committee fully expects the SBA to make use of existing information and materials, where appropriate, to carry out the activities of the Small Business Computer Security and Education Program. Within the Federal government, there already exists the Institute for Computer Sciences and Technology (ICST) as part of the National Bureau of Standards within the Department of Commerce. For more than 10 years, ICST has been helping organizations use computer and network technologies more effectively. ICST sponsors and participates in conferences, workshops, and meetings to share information and provide advice. ICST has also published and disseminated articles on best practices for computer security. However ICST is not mandated to serve small businesses directly and currently can not use regular program funds for this purpose. The Committee amendment does require the SBA to consult with ICST and utilize their expertise to develop or adapt already existing information and materials for the "Small Business Computer Security and Education Program."

B. PRIVATE SECTOR COOPERATION

The SBA is currently prohibited from cooperating with profit-making organizations in providing counseling, training, and other types of management assistance. In the Committee hearing, the Administration testified that in the fields of computer technology and communications, almost all the expertise is concentrated in profit-making firms. According to Mr. James Thomson, Associate Administrator for Management Assistance of the Small Business Administration, "access to the revolution in information science may make the difference in survival or failure of many small businesses."

Currently, section 8(b) of the Small Business Act provides for technical and managerial aid to small business concerns "by cooperating and advising with voluntary business, professional, educational, and other nonprofit organizations, associations, institutions and with other Federal and State agencies . . ."

This section is the basis for the Management Assistance Division's Cosponsored Training program, wherein "voluntary nonprofit" organizations and institutions present small business management training to the small business community at a nominal fee and during hours that make it easy for the business community to attend.

The cosponsored training program is a highly leveraged program, utilizing minimum budget funds from the Agency. This vital program has been one of SBA's most successful outreach programs, but there is still a significant gap between the need for this training and the Agency's ability to fill that need.

On May 4, 1983, Senator Weicker introduced, at the agency's request, legislation (S. 1203) to permit the SBA to utilize profitmaking organizations in providing management assistance to small businesses. The Committee amendment incorporates the legislation.

The capacity of the private sector to provide this kind of assistance has great potential. For example, profit-oriented businesses, particularly in the high technology sector, possess knowledge and expertise in areas not currently available through the voluntary, nonpofit organizations SBA is authorized to use. Utilization of the private sector for training of small business owners and potential small business owners would unlock large areas of knowledge for the small business community not now available to them.

The Agency indicated that it is currently reaching over 350,000 of the more than 13 million small businesses of the Nation with the transfer of knowledge of good business practices. According to the SBA, the amendment to this section of the Small Business Act to permit the development of training programs with the private sector would more than triple the agency's training capacity at no increase in Government cost.

However, the Committee strongly believes that the Federal government should not appear to endorse particular products or services of these for-profit concerns. The authority given to the Small Business Administration to cosponsor training with profitmaking groups should be strictly controlled. Before any cosponsored events are undertaken, the program and the cosponsor could be expected to enter into a written agreement to define clearly the cosponsorship terms. The Committee amendment requires the Administration to take such actions as it determines to be necessary to avoid the undue promotion of the products or services of any such profitmaking concern.

This new authority for SBA should have a dual benefit. It should reduce the agency costs and improve the linkage between the private sector and the Federal government in the delivery of current knowledge on computer technology, communications, and management assistance to the small business community.

C. ADVISORY COUNCIL

The Committee believes that no one group has a full grasp of computer crime problems as it affects the small business community and that the expertise concerning computer technology and computer security is spread across many different disciplines in both the public and private sector. In the Committee view, the Small Business Administration would benefit from the advice of computer technology and computer security experts from both of these sectors in developing and implementing the "Small Business Computer Security and Education Program." Therefore, the Committee amendment has replaced the proposed task force and study of issues with an advisory council encompassing many of the same goals and multiplying the sources for advice.

The Advisory Council would consist of an employee of each of the following four departments who would be named by the Department head: the Small Business Administration, the Institute for Computer

Sciences and Technology of the Department of Commerce, the Department of Justice and the Department of Defense. The Advisory Council would also consist of five other members appointed by the Administrator of the SBA, and who would be representative of each of the following groups: the providers of computer hardware to small business, the providers of computer software to small business, the providers of liability insurance to small business computer users, the providers of computer security services to small business, and the associations representing small business concerns. In addition, the Administrator would be authorized to appoint such other members from the private sector to the Advisory Council as he deemed appropriate.

The Advisory Council is required to meet at least annually or more frequently at the request of the Administrator. The meetings of the Advisory Council should provide SBA, and those with a major interest in the prevention of computer crime, a forum for the exchange of ideas and information and a structure to focus on comprehensive solutions to the problem of computer security.

The bill also provides that the Council advise SBA on the development and implementation of a common sense computer security and education program that will substantially benefit small businesses.

The Advisory Council should be able to identify existing resources that would benefit small business computer users and facilitate the involvement of the private sector with the SBA's computer security and education program.

IV. SECTION-BY-SECTION ANALYSIS

The Committee amendment consists of seven sections, the first of which identifies the title of the Act as the "Small Business Computer Security and Education Act of 1984."

Section 2(a) of the Committee amendment contains Congressional findings that there is an increased dependency on information technology, including computers, in the small business community; that such technology has permitted and expanded criminal activity against small businesses, that small businesses are not always able to protect their information technology from unauthorized use; that there is substantial expertise with profitmaking organizations concerning computer technology, communications, and management assistance that is not available in the nonprofit arena; and that use of such expertise would help improve substantially the management assistance program of the Small Business Administration.

The bill's stated purposes are to improve small business management of their information technology and to encourage them to protect such technology from criminal activity. An additional purpose of the bill is to allow the Small Business Aministration to cooperate with profitmaking as well as nonprofitmaking organizations in providing management assistance to small business.

Section 3 would direct the Administrator of the Small Business Administration, within 90 days of enactment, to establish a "Computer Security and Education Advisory Council." The Advisory Council would consist of an employee of each of the following four departments who would be named by the Department head: the Small Busi-

ness Administration, the Institute of Computer Sciences and Technology of the Department of Commerce, the Department of Justice and the Department of Defense. The Advisory Council would also consist of five other members appointed by the Administrator of the SBA, and who would be representative of each of the following groups: the providers of computer hardware to small business, the computer software to small business, the providers of liability insurance to small business computer users, the providers of computer security services to small business, and the associations representing the general interests of small business concerns. In addition, the Administrator would be authorized to appoint to the Advisory Council such other members from the private sector as he deemed appropriate.

Section 3(c) defines the functions of the Advisory Council to include providing advice to the Administrator on the nature and scope of computer crimes committed against small businesses; the effectiveness of Federal and State law in determining computer-related criminal activity; the effectiveness of computer technology and management techniques available to small business for increasing their computer security; the development of guidelines to assist small businesses in evaluating the security of computer systems; and recommendations for appropriate functions of the "Small Business Computer Security and Education Program" .The Advisory Council shall meet at least annually and at such other times at the request of the Administrator. The Administrator shall designate one of the non-Federal employee members to be chairperson of the Advisory Council. Each member of the Advisory Council shall serve without pay but the non-Federal members shall be reimbursed for actual expenses.

Section 4 of the bill directs the Administrator of the SBA to establish a "Small Business Computer Security and Education Program" to provide to small businesses information regarding the utilization and management of computer technology, computer crimes committed against small businesses, and security for computers owned or utilized by small businesses. The Administrator would also be required to provide for periodic forums for small business concerns to improve the exchange of information regarding these matters and to provide training opportunities to educate small business users on computer security techniques.

This section further stipulates that the Administrator, after consultation with the Director of the Institute of Computer Sciences and Technology, shall develop information and materials to carry out the activities to be offered by the "Small Business Computer Security and Education Program".

Section 5 will allow for the first time the Small Business Administration to cooperate with profitmaking as well as non-profitmaking organizations to improve the quality and scope of the management assistance program being provided to small businesses. The Administrator shall take such actions as is determined to be necessary to avoid undue promotion of the products or services of any such profitmaking organization.

Section 6 defines the term "computer crime" to mean any crime committed against a small business concern by means of the use of a computer and any other crime involving the illegal use of, or tam-

pering with, a computer owned or utilized by a small business concern".

Section 7 stipulates that the Act shall take effect on October 1, 1984, that the statutorily-established Advisory Council will operate for 3 years, and that at the end of this 3-year period, the Administrator may continue the operation of the Advisory Council for a longer period if he so desires.

Matters Required to be Discussed Under Senate Rules

A. COMMITTEE VOTE

On May 8, 1983, the Commmittee met in executive session and, with a quorum present, agreed to favorably report out H.R. 3075, with an amendment in the nature of a substitute, and an amendment to the title.

YEAS	NAYS
Weicker	
Packwood *	
Boschwitz	
Gorton	
Nickles	
Rudman	
D'Amato *	
Kasten *	
Pressler	
Nunn	
Huddleston *	
Sasser *	
Levin *	
Tsongas	
Dixon	

[1] Indicates voted by proxy.

B. COST OF THE LEGISLATION

In compliance with rule XXVI of the Standing Rules of the Senate, the Committee estimates that the cost of the legislation will be equal to the amounts indicated by the Congressional Budget Office in the following letter:

U.S. Congress,
Congressional Budget Office,
Washington, D.C., May 9, 1984.

Hon. Lowell P. Weicker, Jr.,
Chairman, Committee on Small Business, U.S. Senate, Russell Senate Office Building, Washington, D.C.

Dear Mr. Chairman: The Congressional Budget Office has reviewed H.R. 3075, the Small Business Computer Security and Education Act of 1984, as ordered reported by the Senate Committee on Small Business, May 8, 1984.

H.R. 3075 would establish a Small Business Computer Security and Education Advisory Council composed of representatives from the

federal government and the private sector. The council, under the direction of the Administrator of the Small Business Administration (SBA), would meet annually and advise the Administration on a variety of computer crime and security issues which affect small businesses. Council members would serve without pay, but would be reimbursed for actual expenses, including travel. Based on information provided by the SBA, it is estimated that the cost of the task force would be approximately $80,000 in each of the fiscal years 1985, 1986, and 1987. The estimated cost could be somewhat more or less, depending upon the number and location of meetings, as well as the scope of the analysis provided to the Administration. At the discretion of the Administration, the council could continue its functions beyond the sunset date of October 1, 1987. In that case, the estimated annual cost would remain at approximately the same level in each year the council continues its operations.

In addition, H.R. 3075 would require the SBA to establish a small business computer security and education program within SBA to provide small businesses with information regarding computer crimes and safety. Based on information from the SBA, we expect that approximately $100,000 annually would be required to implement this provision beginning in fiscal year 1985.

Enactment of this bill would not affect the budgets of state and local governments.

If you wish further details on this estimate, we will be pleased to provide them.

Sincerely,

ERIC HANUSHEK
(For Rudolph G. Penner, Director).

C. REGULATORY IMPACT STATEMENT

In compliance with rule XXVI(11)(b) of the Standing Rules of the Senate, it is the opinion of the Committee that no significant additional regulatory impact would be incurred in carrying out the provisions of the legislation. Nor does the Committee believe that the bill would have an additional impact on the privacy of companies or individuals participating in the program.

In the opinion of the Committee, enactment of this bill will not result in additional paperwork requirements for the small business sector of the economy.

V. CHANGES IN EXISTING LAW

In compliance with rule XXVI(12) of the Standing Rules of the Senate, changes in existing law made by the statutory provisions of the bill are as follows (existing law proposed to be omitted is enclosed in black brackets, new material is printed in italic, and existing law in which no change is proposed is shown in roman):

SMALL BUSINESS ACT

* * * * * * *

SEC. 3 * * *

(j) For purposes of this Act—

(A) the term 'computer crime' means—

(i) any crime committed against a small business concern by means of the use of a computer; and

(ii) any crime involving the illegal use of, or tampering with, a computer owned or utilized by a small business concern.

* * * * * * *

SEC. 4(b)(2) * * *

"(3)(A) The Administrator shall, not later than ninety days after the effective date of the Small Business Computer Security and Education Act of 1984, establish an advisory council to be known as the Small Business Computer Security and Education Advisory Council (hereinafter referred to as the 'advisory council').

"(B) The advisory council shall consist of the following members:

"(i) an official of the Small Business Administration, appointed by the Administrator;

"(ii) an official of the Institute for Computer Sciences and Technology of the Department of Commerce, appointed by the Secretary of Commerce;

"(iii) an official of the Department of Justice, appointed by the Attorney General, who is knowledgeable about issues of computer security and its prosecution;

"(iv) an official of the Department of Defense, appointed by the Secretary of Defense, who is knowledgeable about issues of computer security;

"(v) individual, appointed by the Administrator, who is representative of the interests of the manufacturers of computer hardware to small business concerns;

"(vi) one individual, appointed by the Administrator, who is representative of the interests of the manufacturers of computer software to small business concerns;

"(vii) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer liability insurance to small business concerns;

"(viii) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer security equipment and services to small business concerns;

"(ix) one individual, appointed by the Administrator, who is representative of the interests of associations of small business concerns, other than small business concerns engaging in any of the activities described in clauses (v) through (viii); and

"(x) such additional qualified individuals from the private sector, appointed by the Administrator, as the Administrator determines to be appropriate.

"(C) It shall be the function of the advisory council to advise the Administration on—

"(i) the nature and scope of the computer crimes committed against small business concerns;

"(ii) the effectiveness of Federal and State law in deterring computer-related criminal activity or prosecuting computer-related crimes;

"(iii) the effectiveness of computer technology and management techniques available to small business for increasing their computer security;

"(iv) the development of information and guidelines to be made available to the Administrator to assist small business concerns in evaluating the security of computer systems; and

"(v) such other appropriate functions of the small business computer security and education program.

"(D) The Administrator shall designate one of the non-Federal members of the advisory council as its chairperson. The advisory council shall meet at least annually and at such other times as requested by the Administrator. A majority of the members of the advisory council shall constitute a quorum. Vacancies on the council shall be filled in the same manner as tne original appointment.

"(E) Each member of the advisory council shall serve without additional pay, allowances, or benefits by reason of such service. Each non-Federal member shall be reimbursed for actual expenses, including travel expenses, as authorized by section 5703 of title 5, United States Code.

"(F) Upon request of the chairperson of the advisory council, the Administrator may request directly from any Federal agency information necessary to enable the advisory council to carry out its functions under the Small Business Computer Security and Education Act of 1984. Upon the request of the Administrator, the head of such agency shall furnish to the Administrator such information, subject to the requirements of section 552 of title 5, United States Code.".

"(4)(A) The Administrator shall establish a small business computer security and education program to—

"(i) provide small business concerns information regarding—

"(I) utilization and management of computer technology;

"(II) computer crimes committed against small business concerns; and

"(III) security for computers owned or utilized by small business concerns;

"(ii) provide for periodic forums for small business concerns to improve their knowledge of the matters described in clause (i); and

"(iii) provide training opportunities to educate small business users on computer security techniques.

"(B) The Administrator, after consultation with the Director of the Institute of Computer Sciences and Technology within the Department of Commerce, shall develop information and materials to carry out the activities described in subparagraph (A) of this paragraph.".

* * * * * * *

SEC. 8. * * *

(b) It shall also be the duty of the Administration and it is hereby empowered, whenever it determines such action is necessary—

(1)(A) to provide technical and managerial aids to small business concerns, by advising and counseling on matters in connection with Government procurement and property disposal and on policies, principles, and practices of good management

including but not limited to cost accounting, methods of financing, business insurance, accident control, wage incentives, *computer security*, and methods engineering, by cooperating and advising with voluntary business, professional, educational, and other nonprofit organizations, associations, and institutions, *with profitmaking concerns*, and with other Federal and State agencies, by maintaining a clearinghouse for information concerning the managing, financing, and operation of small business enterprises, by disseminating such information, and by such other activities as are deemed appropriate by the Administration: *Provided, That the Administration shall take such actions as it determines to be necessary to ensure that the participation by a profitmaking concern does not constitute an endorsement by the Federal Government of the products or services of any such concern, and to avoid the undue promotion of the products or services of any such profitmaking concern, but the mere participation by such concern shall not, in itself, be considered a promotion or endorsement of its products or services ; and*

* * * * * * *

○