

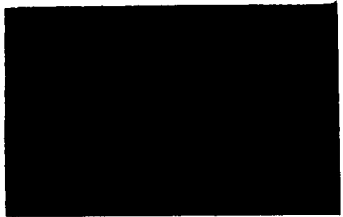
3-1-155

OFFICE OF THE DIRECTOR



Office of Security

2 September 1987



TO: DD/PTS  
C/ISG

SUBJECT: Computer Security Act of 1987

OS REGISTRY  
OS-1287X-87  
4 SEP 1987

Wayne/Susan:

I need to know your concerns. Also share them  
with  Office of Congressional Affairs.

STAT

STAT



Att

Distribution:  
Orig: DD/PTS; C/ISG  
1 - D/Sec  
① - OS Registry



... would write off the Historic Preservation Fund because of the law but the law doesn't help naturally or Government entities and the very law itself depends absolutely of the fund.

The authorization to deposit into the Historic Preservation Fund expires at the end of this fiscal year, on September 30, 1987—less than 130 days from now. H.R. 1744 would simply amend the Historic Preservation Act and extend the authorization for income into the Historic Preservation Fund from 1987 to 1992.

Mr. Speaker, I would be remiss if I did not point out the disappointment of myself and other committee members at the level of appropriation that has been provided especially in recent years under this authority. The administration posture is very disappointing, requesting zero funding year after year, it has therefore been an uphill fight for the Congress to keep even limited funding in place. This is ironic when we look at the important work that we depend on States and local government to do the certification of historic preservation Federal tax credits, the surveys of historic resources and sites, the creation of State historic preservation plans. Some States have even threatened to abandon the cooperative venture because of the national government mandates without the funding commitment justified to help achieve such State fulfilled tasks. Fortunately to date the infrastructure remains intact. As we reauthorize this Historic Preservation Fund hopefully we will recommit ourselves the Congress and the administration to the basic commitment and promise of the 1966 National Historic Preservation Act.

This legislation should be enacted to help ensure that our past will not be lost, now or in the future. Mr. Speaker, I urge adoption of this measure to make certain that the Historic Preservation Act has some fuel in the tank to keep the engine running for at least the next few years.

Mr. MARLENEE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of H.R. 1744, that would extend the authorization of the Historic Preservation Fund through 1992. Rather than listing all the reasons of why this bill should be given approval by this body, let me highlight only one point. This entire bill is only one sentence long and it allows a current program to remain in law until 1992. The administration does not oppose this even though they have recommended zero funding in their last several budgets.

There have been many accomplishments in protecting and keeping our past available for everyone to enjoy. This has been done not only through

... from the private sector... support of State and local government... this program has continued although not in the degree that some would like but in short it's alive and well, but maybe not fat and happy.

Mr. VENTO. Mr. Speaker, I yield myself such time as I may consume and rise to point out this bill enjoys the sponsorship of the gentleman from Arizona [Mr. URALL], chairman of the full committee, and the gentleman from California [Mr. LAGOMARINO], the ranking minority member, on a bipartisan basis.

I want to thank the gentleman from Montana [Mr. MARLENEE] for rising and being in support of this measure. I hope the House will act on this measure.

Mr. MARLENEE. Mr. Speaker, I yield myself such time as I may consume to commend the gentleman from Minnesota [Mr. VENTO] and the gentleman from California [Mr. LAGOMARINO], who has a very great interest in this piece of legislation. I think they have done a superb job with the hearings, and I recommend passage of the legislation.

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

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

Mr. SPEAKER pro tempore. The question is on the motion offered by the gentleman from Minnesota [Mr. VENTO] that the House suspend the rules and pass the bill, H.R. 1744.

The question was taken; and (two-thirds having voted in favor thereof) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

HR 145  
COMPUTER SECURITY ACT OF 1987

Mr. ROE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 145) to provide for a computer standards program within the National Bureau of Standards, to provide for Governmentwide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes, as amended.

The Clerk read as follows:

H.R. 145

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 "Computer Security Act of 1987".

SEC. 2. PURPOSE

(a) IN GENERAL.—The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such sys-

... to ensure the... Federal... responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information and

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

SEC. 2. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM

The Act of March 3, 1901 (15 U.S.C. 2727b), is amended—

(1) in section 21(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu thereof "and", and by inserting after such paragraph the following:

"(20) the study of computer systems (a term as defined in section 20(d) of the Act) and their use to control machinery and processes";

(2) by redesignating section 20 as section 22, and by inserting after section 19 the following new sections:

"Sec. 20. (a) The National Bureau of Standards shall—

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems.

"(2) except as described in paragraph 1 of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code

"(3) have responsibility within the Federal Government for developing technical management, physical and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

"(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code and

"(B) those systems which are protected all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense, foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse.

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation, and

...to assist the private sector, upon request, in using and applying the results of the programs and activities under this section.

(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949.

(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949.

(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987.

(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to derive techniques for the cost effective security and privacy of sensitive information in Federal computer systems; and

(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget) -

(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

(c) For the purposes of - (1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(3) and (a)(5), and (2) performing research and conducting studies under subsection (b)(5), the National Bureau of Standards shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

(d) As used in this section - (1) the term 'computer system' - (A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, move-

...related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949.

(2) the term 'Federal computer system' - (A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function; and (B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949.

(3) the term 'operator of a Federal computer system' means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function.

(4) the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

(5) the term 'Federal agency' has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

SEC. 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom shall be representative of small or medium sized companies in such industries.

(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

(b) The duties of the Board shall be - (1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy.

(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the

...of the Board shall not act in the absence of a quorum, which shall consist of seven members.

(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter 1 of chapter 57 of title 5, United States Code.

(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

(g) As used in this section, the terms 'computer system' and 'Federal computer system' have the meanings given in section 20(d) of this Act; and

(3) by adding at the end thereof the following new section:

SEC. 21. This Act may be cited as the National Bureau of Standards Act.

SEC. 4. AMENDMENT TO BOOKS ACT. Section 111(d) of the Federal Property and Administrative Services Act of 1949 (49 U.S.C. 759(d)) is amended to read as follows:

(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

(2) The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would ac-

The Secretary shall have authority to promulgate regulations to carry out the purposes of this Act, subject to the approval of the Administrator of the Federal Bureau of Investigation, the Administrator of the Federal Reserve System, the Administrator of the Federal Bureau of Prisons, the Administrator of the Federal Bureau of Investigation, the Administrator of the Federal Reserve System, the Administrator of the Federal Bureau of Prisons, the Administrator of the Federal Bureau of Investigation, the Administrator of the Federal Reserve System, the Administrator of the Federal Bureau of Prisons.

(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection.

(5) As used in this subsection, the terms 'Federal computer system' and 'operator of a Federal computer system' have the meanings given in section 20(d) of the National Bureau of Standards Act."

SEC. 6 FEDERAL COMPUTER SYSTEM SECURITY TRAINING

(a) IN GENERAL.—Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be—

(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(b) TRAINING OBJECTIVES.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (a). Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved computer security practices.

(c) REGULATIONS.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

SEC. 7 ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS SECURITY AND PRIVACY

(a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE INFORMATION.—Within 6 months after the date of enactment of this Act, each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

(b) SECURITY PLAN.—Within one year after the date of enactment of this Act, each such

system shall be subject to a security review by the Administrator of the Federal Bureau of Investigation, the Administrator of the Federal Reserve System, the Administrator of the Federal Bureau of Prisons, the Administrator of the Federal Bureau of Investigation, the Administrator of the Federal Reserve System, the Administrator of the Federal Bureau of Prisons, the Administrator of the Federal Bureau of Investigation, the Administrator of the Federal Reserve System, the Administrator of the Federal Bureau of Prisons.

As used in this Act, the terms "computer system", "Federal computer system", "operator of a Federal computer system", and "sensitive information" have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act).

SEC. 8 RULES OF CONSTRUCTION OF ACT.

Nothing in this Act, or in any amendment made by this Act, shall be construed—

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is—

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.

The SPEAKER pro tempore. Pursuant to the rule, a second is not required on this motion.

The gentleman from New Jersey [Mr. ROE] will be recognized for 20 minutes and the gentleman from New York [Mr. HORTON] will be recognized for 20 minutes.

The Chair recognizes the gentleman from New Jersey [Mr. ROE].

Mr. ROE. Mr. Speaker, I yield myself such time as I may consume.

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

Mr. ROE. Mr. Speaker, Members on both sides of the aisle have worked unusually hard on this bill. I particularly want to acknowledge the leadership of MANUEL LOJAN, the ranking Republican of the full committee; DOUG WALGREN and DAVE McCURDY, chairmen of the two subcommittees that dealt with this legislation; and SHERRY BOEHLETT and TOM LEWIS, ranking Republicans of the subcommittees. I would like to pay special tribute to DAN GLICKMAN whose inspiration, and perseverance were the driving forces behind this bill.

Hearings first began nearly 4 years ago in the subcommittee, chaired at that time by Mr. GLICKMAN. Since then, many others, including our colleagues on the Government Oper-

problem facing the country. The bill that the full committee are bringing to the floor today is a culmination of 2 years' work. It represents what I believe is a long-overdue step toward solving a growing problem, one brought about by our ever-increasing dependence on computer systems. It is no secret that society—and especially the Government—has become highly dependent on computers and the enormous quantities of information they contain. Yet the low level of protection given to this information, in most cases, makes it vulnerable to all kinds of abuse.

I believe these steps will go a long way toward protecting the vast array of information with which we entrust the Federal Government. For example, the committee received testimony that computer fraud and abuse cost the Government an estimated \$1 billion each year, largely because of inadequate safeguards in various financial and benefit systems. Another area that concerns me greatly is the integrity of air traffic control information. The FAA absolutely depends on these data to keep airplanes from colliding in the skies. Yet there is very little protection from the possible criminal action of a disgruntled person. Although unlikely, the consequences of such action could be a major air disaster. We simply must take reasonable precautions to assure the integrity of this information.

H.R. 145 accomplishes two objectives that will lead to much greater security of Federal computer systems. First, it calls for improved training of Federal workers in good computer security practice. And it provides a strengthened focal point for developing policy and guidance for the civil agencies.

Mr. Speaker, these provisions of this bill were worked out over many months and with great care. I believe we have a strong consensus among both committees that the bill is a practical and cost-effective approach. I recommend its adoption.

□ 1320

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

Mr. HORTON. Mr. Speaker, I yield myself 5 minutes.

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

Mr. HORTON. Mr. Speaker, I rise in strong support of H.R. 145, the Computer Security Act of 1987. This legislation is the product of many months of negotiations between the Government Operations and Science Committees, on the one hand, and the administration on the other. I believe we have fashioned a good, workable bill worthy of the support of all of the Members.

Many people deserve credit for putting this bill together. The chairman

...the Chairman of the Committee on Science and Technology, Sub Panel, the ranking minority member of the Science Committee, MARVIN LUTAN and, of course, Congressman DAN GLICKMAN and the original sponsor of this legislation.

I also would like to include in that list the White House Chief of Staff Howard Baker, National Security Advisor Frank Carlucci, Secretary of Commerce Malcolm Baldrige, Deputy Secretary of Defense William Taft, and Office of Management and Budget Director Jim Miller.

They worked hard and made it possible for us to bring this landmark legislation to the floor and I think we can all be proud of our work in this matter.

Mr. Speaker, H.R. 145 assigns to the National Bureau of Standards responsibility for developing standards and guidelines to assure the cost-effective security and privacy of sensitive, non-classified information in Federal computer systems. There is no question of the need for a prudent tightening of computer security in the Federal Government. The legislation responds to this need by requiring the establishment of security plans by all operators of Federal computer systems. It also mandates periodic training in accepted computer security practice for all persons involved in the management, use, or operation of those systems.

This bill is directed toward sensitive computer information such as Social Security, tax, and census records. There is a pressing need to control loss and unauthorized modification or disclosure of sensitive information in such systems, both to protect personal privacy and to prevent computer-related fraud and abuse.

I want to note that H.R. 145 applies only to computer systems which do not contain classified information. This allows the defense and intelligence communities to meet their specific computer security needs in whatever manner is appropriate for them.

I have mentioned that H.R. 145 is the product of negotiations that led to a compromise acceptable to all sides. The main point of controversy was which agency in the Government should have primary responsibility for setting computer security standards for systems which contain unclassified information. The National Security Agency has great expertise in the area of computer security, but that expertise is narrowly focused to meet intelligence and national security needs. The Government Operations Committee, the Science, Space and Technology Committee, and the administration have all concluded that the security responsibility for setting security

standards in the business world, and I deal regularly with a wide range of computer equipment vendors. It is best able to do the job called for in H.R. 145.

The compromise directs NBS to develop the Governmentwide standards and guidelines, drawing upon the work of the National Security Agency, where it is consistent with the requirements of unclassified systems. The National Security Agency has a role with regard to standards or guidelines, but it is advisory to NBS. Clearly, these two agencies must work together if the Government is to take full advantage of the technical resources which are available between them. However, it is my belief—and one shared by both committees—that the National Bureau of Standards must be the clear leader when we are dealing with civilian programs.

Mr. Speaker, enactment of H.R. 145 will establish a framework for correcting the defects and lapses in our current means of securing Government civilian computer systems. The bill is supported by the administration, White House and agency officials worked closely with both the Committee on Government Operations and the Committee on Science, Space, and Technology to achieve this compromise version. I urge its adoption.

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

Mr. ROE. Mr. Speaker, I yield such time as he may consume to the distinguished chairman of the Committee on Government Operations, the gentleman from Texas, Mr. JACK BROOKS.

Mr. BROOKS. Mr. Speaker, as chairman of the Committee on Government Operations, I rise in full support of the Computer Security Act of 1987. I want to commend Chairman ROE, Congressman GLICKMAN, and the other members of the Science, Space, and Technology Committee for their excellent work on this legislation. During the 3 days of hearings held by the Government Operations Committee, we found that a strong computer security program was urgently needed to protect the Government's computerized data bases from unauthorized manipulation and potential destruction.

Current estimates from the Office of Technology Assessment indicate that over \$60 billion is spent annually by Federal agencies to acquire, develop, and use information technology. While it has greatly increased the efficiency of Government programs, information technology has also made the agencies vulnerable to outside penetration by criminal or foreign elements.

H.R. 145 would correct this problem by increasing the awareness of the critical importance of computer security

standards and guidelines to defend against unauthorized access to vital Government information and for mandatory training of Federal employees.

In addition, H.R. 145 would require NBS to create a Computer Security Board composed of experts from the Government and the private sector. The bill also makes it clear that nothing in this act will affect the release of information as required under the Freedom of Information Act or other laws.

During the committee's consideration of the bill, concerns were raised by a wide range of witnesses that actions by a few DOD officials under national security decision directive 145 and the Poindexter directive were leading to "Big Brotherism." To allay these concerns, we worked with the administration to ensure that a civilian agency, NBS, would be in charge of this important program.

I am pleased to say that, as a result of our joint efforts, the administration has given its full support to the passage of the bill. I urge all Members to do likewise and vote in favor of the Computer Security Act of 1987.

I also request permission to include at the close of my comments a letter from the very able Director of the Office of Management and Budget, Jim C. Miller III, on this very subject in which he agrees with the substance of this legislation and he adds the fact, which we all ought to be aware of, that the National Security Agency will be utilized and will be drawn upon to give available technical information to the National Bureau of Standards as a workout of these guidelines. They are not obligated to do that. Mr. Miller points that out. It is advisory, subject to the appropriate national board of a standards review.

The text of the letter referred to is as follows:

OFFICE OF MANAGEMENT AND BUDGET,  
Washington, DC, May 12, 1987.

HON. JACK BROOKS,  
Chairman, Committee on Government Operations,  
House of Representatives,  
Washington, DC.

DEAR MR. CHAIRMAN: I am pleased that through intensive consultations between the Administration and the Congress great progress has been made toward agreement on a Computer Security Act of 1987. I hope that this statement of administration views will assist in offering construction solutions to areas where further improvements are desirable.

As we have reviewed H.R. 145, a primary concern has been to assure that roles of the National Bureau of Standards (NBS), and the National Security Agency (NSA) are discharged in a manner that will promote a sound public policy and result in efficient, cost effective, and productive solutions. In this regard it is the Administration's position that NBS, in developing Federal stand-

... and in some cases, the  
best government action is to do nothing. We  
believe this would avoid unnecessary duplication  
of effort.

Computer security standards, like other  
computer standards, will be developed in ac-  
cordance with established NSB procedures.  
In this regard, the technical security guide-  
lines provided by NSA to NBS will be treated  
as advisory and subject to appropriate  
NSB review. In cases where civil agency  
needs will best be served by standards that  
are not consistent with NSB technical  
guidelines, the Secretary of Commerce will  
have authority to issue standards that best  
satisfy the agencies' needs. At the same  
time, agencies will retain the option to ask  
for Presidential review of standards issued  
by the Department of Commerce which do  
not appear to be consistent with U.S. public  
interest, including that of our national security.  
I am enclosing proposed changes to the  
present text of H.R. 145 which are consistent  
with the NBS-NSA relationship outlined  
above and make several minor changes that  
would further improve the bill.

In closing, I want to assure you that a re-  
ported bill within the parameters outlined  
in this letter will have the Administration's  
support.

Sincerely yours,

JAMES C. MILLER III  
Director

Mr. HORTON, Mr. Speaker, I yield 5  
minutes to the gentleman from New  
Mexico, Mr. MANUEL Lujan, the ranking  
minority member of the Committee  
on Science, Space, and Technology,  
one of the principal architects of  
this legislation.

I would like to take this opportunity  
to commend the gentleman for his  
fine leadership on this legislation.

Mr. LUJAN, I thank the gentleman  
for yielding me this time and for those  
kind remarks.

Mr. Speaker, I rise in support of  
H.R. 145, as amended by the Science,  
Space, and Technology Committee.  
This bill is the product of extensive  
negotiations with the Administration,  
the Committee on Government Opera-  
tions and the Science Committee.  
H.R. 145 seeks to focus the civil ag-  
encies' attention on the need for comput-  
er security training and cost-effective  
procedures for protecting sensitive  
Government information from unau-  
thorized uses.

I have expressed strong reservation,  
in the past, with various provisions in  
the bill, as introduced. The bill estab-  
lished within the National Bureau of  
Standards (NBS) the authority to de-  
velop computer security guidelines and  
standards for civil agencies. I feel  
strongly that this should be done with  
full knowledge and review of any and  
all existing Federal efforts in this  
area. Whether it be within the classi-  
fied community, or not, substantial  
taxpayer dollars have gone toward cre-  
ating a wealth of technical informa-  
tion on computer security measures.

... and in some cases, the  
best government action is to do nothing. We  
believe this would avoid unnecessary duplication  
of effort.

To further enhance intra-Federal co-  
operation, the 10th National Comput-  
er Security Conference, sponsored by  
NSA and NBS, will be held September  
21-24, 1967. The theme of this year's  
conference is "Computer Security—  
from Principles to Practices." This  
conference should assist in bringing  
together not only Federal agencies,  
but also State and local governments,  
the private sector and academia in a  
setting that encourages the sharing of  
technical information and expertise.

Mr. Speaker, this bill addresses the  
need to secure sensitive information.  
This is distinct from information that  
is clearly under the classified umbrella.  
Nevertheless, there may be in-  
stances when a Federal agency or a  
Federal computer system may involve  
the use of classified and nonclassified  
information. Under such circum-  
stances, H.R. 145 gives authority to  
agency heads to elect the more secure  
standards, so as to eliminate the need  
for dual security procedures.

As the fine points of this legislation  
have been worked out over the last  
several months, I urge my colleagues  
to support passage of this legislation. I  
believe it will assist in raising comput-  
er security procedures "up the ladder"  
of priorities in the Federal civilian  
agencies.

Mr. ROE, Mr. Speaker, I yield 2 min-  
utes to the gentleman from Kansas  
(Mr. GLICKMAN).

□ 1325

Mr. GLICKMAN, Mr. Speaker, the  
bill before us today is the product of 2  
year's work by two committees, as well  
as the leadership provided by the gen-  
tleman from New Jersey (Mr. ROE),  
the gentleman from Texas (Mr.  
BROOKS), the gentleman from New  
York (Mr. HORROW), and the gen-  
tleman from New Mexico (Mr. LUJAN).

All of these gentlemen deserve a  
great deal of praise today for getting  
this bill to the floor.

The need for H.R. 145 was first  
identified in hearings held almost 4  
years ago. At that time, we noted that  
the Federal Government had become  
totally dependent on automated infor-  
mation systems to perform a multi-  
tude of essential services. Further-  
more, the information stored in Gov-  
ernment computers and transmitted  
over various communications networks  
is vulnerable to unauthorized access  
and disclosure. Fraudulent manipula-  
tion, and disruption. The situation was

... and in some cases, the  
best government action is to do nothing. We  
believe this would avoid unnecessary duplication  
of effort.

Of particular concern was the level  
of security training among people  
who operate, use and manage comput-  
ers. Such people are extremely impor-  
tant in a security sense because, as  
studies have shown, they are the  
greatest problem. It is not the smash  
publicized hacker, working to pen-  
etrate from the outside. Rather, it is  
the insider, the one who already has  
authorized, that causes the greatest  
damage in practice.

Yet, as we learned from GAO's  
survey of 26 computer systems, there  
is very little formalized effort made to  
reach these individuals, to make them  
aware of system vulnerabilities and  
the importance of embracing security.

The purpose of H.R. 145 is to  
strengthen this link. It does this by es-  
tablishing a research program at the  
National Bureau of Standards aimed  
at developing guidance for use by  
agencies in structuring computer secu-  
rity awareness training programs for  
their employees. It also requires that  
such training be given periodically in  
each agency.

The bill also establishes a focal point  
within the Government for developing  
computer system security standards  
and guidelines to protect unclassified,  
but sensitive information. The organi-  
zation location of this focal point is  
the National Bureau of Standards.  
The need for this provision was precipi-  
tated by National Security Decision  
Directive 145, a directive issued by the  
President about 3 years ago. The pur-  
pose of NSDD-145 was to deal broadly  
with Government computer security, a  
widely recognized problem. The imple-  
menting means is an interagency com-  
mittee invested with the authority to  
issue Governmentwide policy and  
guidance.

Both committees held hearings on  
the implications of NSDD-145. Both  
concluded that although there is a  
clear need for better centralized lead-  
ership in this area, the particular for-  
mula in NSDD-145—which favors the  
military—is inappropriate for handling  
civilian needs. For this reason, H.R.  
145 establishes a civil counterpart to  
develop policy and guidance for pro-  
tecting unclassified, sensitive informa-  
tion.

Mr. Speaker, I believe we have  
ample evidence of a disaster waiting to  
happen in the Federal sector. I think  
virtually all Members agree with the  
need to strengthen our overall posture  
in the computer security area. I also  
feel we have an acceptable and cost ef-  
fective vehicle for dealing with the  
problem. I urge passage of H.R. 145.

Mr. Speaker, before I close, in addi-  
tion to thanking the Members that I  
did today, I wish to thank the major-

...from the Committee on Government Operations who also deserve that kind of praise, as well as other staff members in the Committee on Science, Space, and Technology, so with that, Mr. Speaker, I urge passage of the bill.

Mr. WALGREN. Mr. Speaker, I rise in support of H.R. 145, the Computer Security Act of 1987. This measure, which assures civilian control of the computer systems of civilian programs, is the result of much hard work on the part of the Committee on Government Operations. The Subcommittee on Transportation, Aviation, and Materials, and my own Subcommittee, Science, Research and Technology. I want to compliment Mr. GLUCKMAN, the original author of the bill, who has persevered in bringing this most important issue to the attention of the House, as well as the ranking Republican member of the full committee, Mr. LUJAN, for the input and insight he has added to this bill. I also want to express appreciation to the administration for the flexibility and spirit of compromise they have shown in helping to craft a measure which is fair, equitable, and acceptable to all interested parties.

Recent studies by the Government Accounting Office and other agencies have shown that financial losses due to computer-related fraud run into the billions of dollars. Regrettably, our Government has a history of providing adequate security only for computers processing classified data. Computers in the civilian agencies remain vulnerable to knowledgeable outsiders, known as hackers, as well as to disgruntled or unhappy employees. Therefore, the well-designed, effective security program, provided for in this legislation, is badly needed.

In 1983, a report by the Department of Health and Human Services on computer fraud in various Federal agencies reviewed 103 cases of computer abuse and 69 cases of computer fraud. The average theft was \$117,000 and involved low-level employees. Computer abuse typically involved using a Federal computer for outside business or entertainment. Even rudimentary security precautions would have prevented most of these crimes.

H.R. 145 addresses these security problems. The measure assigns the National Bureau of Standards (NBS) the responsibility for developing, with the help of the National Security Agency, standards and guidelines, for the cost-effective security and privacy of sensitive information in unclassified Federal computer systems. The bill also requires all operators of Federal computer systems that contain sensitive information to establish computer security plans. Furthermore, it mandates periodic training sessions, administered by the Office of Personnel Management (OPM), for all Government and Government contractor employees who manage, use, or operate these computers. Let me emphasize that H.R. 145 assures civilian control over computers in Federal civilian agencies.

Mr. HORTON. Mr. Speaker, I commend the bill; it is a landmark piece of legislation.

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

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

The SPEAKER pro tempore (Mr. GRAY of Illinois). The question is on the motion offered by the gentleman from New Jersey [Mr. ROE] that the House suspend the rules and pass the bill, H.R. 145, as amended.

The question was taken; and (two-thirds having voted in favor thereof) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

#### GENERAL LEAVE

Mr. ROE. I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks on H.R. 145, the bill just passed.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from New Jersey?

There was no objection.

#### CONGRATULATIONS TO MONTANA U.S.A. WRESTLING TEAM

(Mr. MARLENEE asked and was given permission to address the House for 1 minute.)

Mr. MARLENEE. Mr. Speaker, we have with us today the Montana U.S.A. Wrestling Team.

Tomorrow this team, after much long and arduous training and practice, will be traveling to the Soviet Union; and there they will be challenged by teams from all over the Soviet Union.

They are our ambassadors. They are clean cut, vigorous youths of Montana and of this Nation, and we are proud of them.

I wish them well when they go over there. The Russians are hard to pin, but I hope that you pin them down and come back with some medals.

Congratulations to the team.

Mr. MOODY. Mr. Speaker, Secretary Shultz recently said that he had no intention of "passing the hat" among U.S. allies for financial help in keeping shipping lanes open in the Persian Gulf.

On June 13, Secretary Shultz told the Los Angeles Times: "The idea of the United States going around (abroad) getting contributions for the support of our Navy just has no appeal."

Mr. Speaker, contrast the Secretary's remarks here with the record of his top aide, Elliot Abrams, of actively and vigorously soliciting contributions abroad for the Nicaraguan Contras.

Secretary Abrams, as we all now know, traveled to London under an assumed name to meet with the Sultan of Brunei and provide account numbers for Colonel North's Swiss bank accounts. Then he fled to Congress about it.

I am concerned that this administration, and particularly Secretary Shultz, wants to go along when the activity is legal, as in the Persian Gulf, without seeking the active commitment and cooperation of our allies. But when the administration wants to conduct foreign policy clearly in conflict with the will of Congress and our country's laws, as in Central America, it finds our foreign friends convenient sources of funds.

Apparently, passing the hat to carry out foreign policy is OK if the activity is illegal, but it is not if it is legal.

This double standard shows disdain for our allies and contempt for Congress at a time when the administration badly needs the support and cooperation of both.

The Los Angeles Times article referred to:

[From the Los Angeles Times, June 13, 1987]

#### U.S. WON'T PASS THE HAT FOR PATROLS IN GULF, SHULTZ SAYS

ANCHORAGE, ALASKA—Secretary of State George P. Shultz, in an implied rebuke to congressional critics of Administration policy on the Persian Gulf, said Friday that the United States has no intention of seeking funds from Japan or nations in Western Europe to pay part of the cost of keeping the gulf open to shipping.

Shultz on the first leg of a 7,575-mile flight from a North Atlantic Treaty Organization foreign ministers meeting in Iceland to talks in the Philippines, said. "The idea of the United States going around getting contributions for the support of our Navy just has no appeal. We don't have to do that."

Shultz spoke to reporters before his aircraft made a refueling stop at Elmendorf Air Force Base near Anchorage.