PROJECTED REDUCTIONS IN DEFENSE PROGRAM—MESSAGE FROM THE PRESIDENT OF THE UNITED STATES (H. DOC. NO. 99-230)

The SPEAKER pro tempore laid before the House the following message from the President of the United States; which was read and, without objection, referred to the Committee on Armed Services and the Committee on Foreign Affairs, and ordered to be printed:

(For message, see proceedings of the Senate of today, Tuesday, June 3, 1986.)

COMMUNICATION FROM CHAIRMAN OF COMMITTEE ON VETERANS' AFFAIRS

The SPEAKER pro tempore laid before the House the following communication from the chairman of the Committee on Veterans' Affairs; which was read and, without objection, referred to the Committee on Appropriations:

COMMITTEE ON VETERANS' AFFAIRS,
Washington, DC, May 21, 1986.

Hon. THOMAS P. O'NEILL,
The Speaker, House of Representatives, Washington, DC.

DEAR MR. SPEAKER: Section 5004 of title 38, United States Code, requires that the Committees on Veterans' Affairs adopt a resolution approving major medical construction projects and leases of $500,000 or more proposed by the Veterans' Administration for each fiscal year. The House Committee on Veterans' Affairs met on May 21, 1986, and authorized the construction of various projects in Fiscal Year 1987 by unanimous voice vote.

A copy of the Resolution adopted by the Committee and a listing of the projects authorized are enclosed.

Sincerely yours,
G.V. (SONNY) MONTGOMERY,
Chairman.

There was no objection.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to the provisions of clause 5 of rule I, the Chair announces that he will postpone further proceedings today on each motion to suspend the rules on which a recorded vote or the yeas and nays are ordered, or on which the vote is objected to under clause 4 of rule XV.

Such rollcall votes, if postponed, will be taken on Wednesday, June 4, 1986.

COMPUTER FRAUD AND ABUSE ACT OF 1986

Mr. HUGHES. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4718) to amend title 18, United States Code, to provide additional penalties for fraud and related activities in connection with access devices and computers, and for other purposes, as amended.

The Clerk read as follows:

H.R. 4718

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 Fraud and Abuse Act of 1986".

SEC. 2. SECTION 1030 AMENDMENTS.

(a) MODIFICATION OF DEFINITION OF FINANCIAL INSTITUTION.—Section 1030(a)(2) of title 18, United States Code, is amended—

(1) by striking out "knowingly" and inserting "intentionally" in lieu thereof; and

(2) by striking out "as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.),".

(b) MODIFICATION OF EXISTING GOVERNMENT COMPUTERS OFFENSE; USE OF COMPUTER EXCLUSION.—Section 1030(a) of title 18, United States Code, is amended—

(1) in paragraph (3), by striking out "knowingly" and inserting "intentionally" in lieu thereof;

(2) in paragraph (3), by striking out ", or having accessed" and all that follows through "prevents authorized use of, such computer";

(3) in paragraph (3), by striking out "if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation" and inserting in lieu thereof "if such computer is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, if such computer is used by or for the Government of the United States and such conduct affects such use"; and

(4) by striking out "It is not an offense" and all that follows through "use of the computer.".

(c) MODIFICATION OF AUTHORIZED ACCESS ASPECT OF OFFENSES.—Paragraphs (1) and (2) of section 1030(a) of title 18, United States Code, are each amended by striking out ", or having accessed" and all that follows through "does not extend" and inserting "or exceeds authorized access" in lieu thereof.

(d) NEW OFFENSES.—Section 1030(a) of title 18, United States Code, is amended by inserting after paragraph (3) the following:

"(4) Knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

"(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters information in that computer, or prevents authorized use of that computer, and thereby causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

"(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

"(A) such trafficking affects interstate or foreign commerce; or

"(B) such computer is used by or for the Government of the United States;".

(e) ELIMINATION OF SECTION SPECIFIC CONSPIRACY OFFENSE.—Section 1030(b) of title 18, United States Code, is amended—

(1) by striking out "(1)"; and

(2) by striking out paragraph (2).

(f) PENALTY AMENDMENTS.—Section 1030 of title 18, United States Code, is amended—

(1) by striking out "(b)(1)" and inserting "(b)" in lieu thereof;

(2) by striking out "of not more than the greater of $10,000" and all that follows through "obtained by the offense" in subsection (c)(1)(A) and inserting "under this title" in lieu thereof;

(3) by striking out "of not more than the greater of $100,000" and all that follows through "obtained by the offense" in subsection (c)(1)(B) and inserting "under this title" in lieu thereof;

(4) by striking out "or (a)(3)" each place it appears in subsection (c)(2) and inserting ", (a)(3), or (a)(6)" in lieu thereof;

(5) by striking out "of not more than the greater of $5,000" and all that follows through "created by the offense" in subsection (c)(2)(A) and inserting "under this title" in lieu thereof;

(6) by striking out "of not more than the greater of $10,000" and all that follows through "created by the offense" in subsection (c)(2)(B) and inserting "under this title" in lieu thereof;

(7) by striking out "not than" in subsection (c)(2)(B) and inserting "not more than" in lieu thereof;

(8) by striking out the period at the end of subsection (c)(2)(B) and inserting "; and" in lieu thereof; and

(9) by adding at the end of subsection (c) the following:

"(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.".

(g) CONFORMING AMENDMENTS TO DEFINITIONS PROVISION.—Section 1030(e) of title 18, United States Code, is amended—

(1) by striking out the comma after "As used in this section" and inserting a one-em dash in lieu thereof;

(2) by aligning the remaining portion of the subsection so that it is cut in two ems and begins as an indented paragraph, and inserting "(1)" before "the term";

(3) by striking out the period at the end and inserting a semicolon in lieu thereof; and

(4) by adding at the end thereof the following:

"(2) the term 'Federal interest computer' means a computer—

"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects such use; or

"(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

"(3) the term 'State' includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;

"(4) the term 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank system and any home loan bank;

"(F) any institution of the Farm Credit System under the Farm Credit Act of 1971; and

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934.

"(5) the term 'financial record' means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution; and

"(6) the term 'exceeds authorized access' means to access a compute with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.".

(h) LAW ENFORCEMENT AND INTELLIGENCE ACTIVITY EXCEPTION.—Section 1030 of title 18, United States Code, is amended by adding at the end the following new subsection:

"(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.".

The SPEAKER pro tempore. Is a second demanded?

Mr. SHAW. Mr. Speaker, I demand a second.

The SPEAKER pro tempore. Without objection, a second will be considered as ordered.

There was no objection.

The SPEAKER pro tempore. The gentleman from New Jersey [Mr. HUGHES] will be recognized for 20 minutes and the gentleman from Florida [Mr. SHAW] will be recognized for 20 minutes.

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

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

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

Mr. HUGHES. Mr. Speaker, I have moved to suspend the rules and pass the bill, H.R. 4718, the Computer Fraud and Abuse Act of 1986. It is with great pleasure and satisfaction that I rise in support of the bill before us. It was reported by voice vote by the Committee on the Judiciary on May 6, 1986. It is the culmination of 4 years of bipartisan work in the Congress.

During this thorough investigation it became clear that computer technology has brought us a long way in the past decade. However, computer technology—with all its gains—has left us with a new breed of criminal: The technologically sophisticated criminal who breaks into computerized data files. One element of this expanding group of electronic trespassers—the so-called hacker—is frequently glamorized by the media, perhaps because the image of the hacker is that of a bright, intellectually curious, and rebellious youth—a modern-day Huck Finn. The facts are these young thrill seekers are trespassers, just as much as if they broke a window and crawled into a home while the occupants were away. The hacker of today can become the white-collar crime superstar of tomorrow, and we must not glamorize our Huck Finns into John Dillingers.

While we need to be concerned about youthful hackers, they pale in significance in comparison to the computer sophisticated criminal who combines his technological skill with old-fashioned greed and criminal intent to rob banks or destroy business records or steal trade secrets. The tools of the trade are not Smith and Wesson, but IBM and Apple. However, in today's world of instant electronic transfer of funds, the result can be more far reaching—and harder for law enforcement to reach.

What can be done about these crimes? I believe government and industry have a dual responsibility: Industry must work to prevent such crimes, and government must be willing and able to prosecute when crimes occur. The legislation before us, I believe, will go a long way toward fulfilling the responsibility of Congress in this scenario.

At this juncture, I would like to bring special attention to my colleagues who have worked hard and effectively in this endeavor. The first is the gentleman from Florida, Mr. NELSON, who was the first to bring this subject to the attention of the House of Representatives and has been a constant champion and dedicated proponent of this important legislation. Also, the ranking Republican of the Subcommittee on Crime, Mr. MCCOLLUM, and Mr. SHAW, who have been invaluable in this bipartisan endeavor. I also would like to thank Senators TRIBLE and LAXALT for their assistance in developing this consensus bill. I appreciate their efforts in shepherding S. 2281, the companion bill to H.R. 4718, in the other body.

As many Members may recall, in the last Congress we enacted computer crime legislation as a part of the conference on the comprehensive crime bill. At the behest of our colleagues in the other body, we deleted from that legislation certain provisions of the House-passed credit card/computer crime bill dealing with felony theft and private-sector offenses involving misuse or damage involving computers. Since that time, both through the hearing process and informal negotiations with interested parties, we have attempted to develop a bill to perfect the existing law and fill the gaps we left as a result of that conference agreement.

The legislation before us today, I believe, will expand in an appropriate but limited manner the types of criminal misconduct involving computers that should be subject to Federal jurisdiction while at the same time leaving to State and local agencies their proper role in this national problem.

In doing so, this bill expands the existing protection of financial records in financial institutions to all customers rather than only to customers who are "individuals" or partnerships consisting of five or fewer partners. The bill would also delete coverage of authorized users of government computers from this portion of existing law and make subsection 1030(a)(3) a pure trespass provision. The improper modifications, destructions or disclosures by authorized users of Federal computers however, are presently violations of other laws such as the Privacy Act, trade secrets laws, 18 U.S.C. 1361, et cetera, and there are adequate administrative sanctions that can also be imposed on Federal employees. Government employees also will be subject to the new "intent to defraud" felony offense in 1030(a)(4). This solves a potential problem that the existing law might have a "chilling effect" on "whistleblowers."

The major impact of this bill is in its three new offenses. The first proposes a 5-year felony violation for unauthorized access to a "Federal interest computer" in furtherance of an intent to defraud. These computers are defined as computers used by the Federal Government or by financial institutions, or when the conduct involves computers in different States. The second new offense can be categorized as "a malicious damage" felony violation in regard to Federal interest computers if there is $1,000 or more in damages.

The last new offense is a misdemeanor provision designed to proscribe the conduct associated with "pirate bulletin boards" used by hackers to display passwords to other persons' computers.

Having worked with experts on computer crime over the past several years, I believe the legislation passed in the last Congress along with the bill now being considered combined—with active efforts of industry to safeguard their property—will address the emergence of the computer criminal in our society.

Protection—both through law and technology—can and must be developed for the intangible property—information—which is the lifeblood of computer systems. Unless we act now to secure the "locks" and provide the laws, computer crime will be the crime wave of the next decade.

□ 1235

It is a good bill, and I would be remiss if I did not thank our staff, Ed O'Connell in particular of the majority staff, and Charlene Heydinger of the minority staff, for their work over the past 6 months in developing this consensus legislation.

It is a good bill. It is a bill that I think will be effective in dealing with the computer criminal.

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

The SPEAKER pro tempore. The gentleman from New Jersey [Mr. HUGHES] has consumed 7 minutes.

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

Mr. Speaker, I would like first of all to compliment the chairman of the subcommittee, the gentleman from New Jersey [Mr. HUGHES], as well as the ranking member, the gentleman from Florida [Mr. MCCOLLUM] and my friend and colleague, the gentleman from Florida [Mr. NELSON], for the wonderful job that has been done on this bill, and also to add my congratulations to the members of the staff, as the chairman just did.

Mr. Speaker, The bill before us today, H.R. 4718, will send a strong message to Americans that computer crime is unacceptable and will be strictly punished. The current law regarding persons who access computers without authorization is enhanced by the provisions of this new bill.

H.R. 4718 protects Federal computers, bank computers, and computers used in interstate commerce. The bill provides a model for States to be used in developing local computer crime laws that would cover all other computers.

H.R. 4718 compliments current law by making it a crime to access a computer of the Federal Government or a financial institution. Penalties are also established for accessing a computer with intent to defraud the Federal Government, a financial institution, or a computer accessed by a second computer from a different State. Destruction of these computers is also prohibited. Finally, persons who traffic in the passwords used to gain unauthorized access to Federal Government computers will also be committing a crime.

This bill improves existing law and expands its coverage to include other serious computer crime activities. I urge the adoption of H.R. 4718.

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

Mr. HUGHES. Mr. Speaker, I yield such time as he may consume to the distinguished gentleman from Florida [Mr. NELSON].

Mr. NELSON of Florida. I thank the gentleman for yielding time to me.

Mr. Speaker, what a privilege for me to come to this point after years of interest in this subject matter, so that I can take the well of this House to thank the chairman of this subcommittee for his vision in understanding the problem of computer crime and then being able legislatively to do something about it.

The gentleman from New Jersey, the chairman of the subcommittee, is a man of extraordinary talent in the way that he can work in a bipartisan fashion and the way in which he can work with our colleagues in the other body and with the administration, specifically the Department of Justice, in fashioning a piece of legislation that will now flesh out the skeletal structure that was passed in 1984 into a complete piece of legislation that will become Federal law to address this problem of computer crime.

The gentleman from New Jersey spoke about the fact that we are confronting a new type of criminal today. It is not the kind of criminal who uses the crowbar, but a criminal who uses the computer keyboard, just as much an effective criminal, just as much a person who, in the old Latin term, uses the "mens rea," the criminal intent, and one who can do a great deal more damage than just breaking into the old safes of yesterday, one who can break into national security information, one who can break into the transactions of interstate commerce, one who can break into, indeed, the transactions of international commerce.

So it is a day of joy and happiness for me, after becoming involved with this subject matter 9 years ago when, then a member of the Legislature of the State of Florida, we passed the first computer crime law in the Nation—which then became a model for the other States. Most of the 50 States now have such laws on their books and now, thanks to the gentleman from New Jersey [Mr. HUGHES], the chairman of the subcommittee, and his counterpart in the other body, Senator LAXALT, we will have a law on the Federal books that will give our prosecutors the tools that they need to go after this new, highly sophisticated type of criminal.

I just want to make reference to one other individual, not an individual who is in this body, but to a fellow who was at the time the chairman of the Florida Legislature Criminal Justice Committee, of which I was one of his subcommittee chairmen, who had the vision back in 1977 and 1978 to realize what potential this had for the Nation, and assigned the State legislation to me. His name is Ralph Haben, from Palmetto, FL, who then went on to become the speaker of the Florida House of Representatives. He is the one who had vision and gave me that opportunity to lead that successful legislative effort.

It is a happy day, and I thank the gentleman from New Jersey for his extraordinary leadership.

Today we are concerned with the broad problem of assuring the security and accuracy of computer operations in the financial and business heart of the Nation.

Computer-assisted crime is the way we should refer to this particular type of wrongdoing. But I doubt that the simpler, less accurate term "computer-crime" will disappear from popular reports of the problem.

Nevertheless, what we are talking about is not crimes committed by computers, but crimes committed by people with the assistance of computers. This includes crimes committed by people at a computer keyboard and crimes that take advantage of the ability of computer systems to bypass the human controls that existed in traditional accounting and auditing procedures.

The computer-assisted crime problem poses major difficulties for the future because computers will be increasingly available in our society to assist in whatever work we have to perform, and that means this power tool will be increasingly available for those criminal persons we always seem to have among us.

Computers may not commit crimes—any more than guns commit crimes. But we have to be realistic—there are people who will commit crimes with guns if they are readily available, and there are people who will commit crimes with computers as they become ubiquitous in our society. I doubt, frankly, that we can address the problem of crime by banning either. Americans may not now be as attached to their computers as they are to their guns, but I suspect they will be inseparable before too long.

It has been estimated that there are some 56,000 large general purpose computers and 213,000 smaller business computers in use by American businesses, universities and research organizations. Another 570,000 minicomputers and 2.4 million desktop computers are in use in the private sector.

The Federal Government, particularly the Pentagon and the Bureau of the Census, has many computers—more than 15,000 computers in the entire Federal establishment, including more than 3,000 in the Department of Defense.

I am sure there will be many more computers in government and business, and in our homes and schools, in the years ahead. I have direct experience in my own congressional office where we have a powerful minicomputer—with 256 K of core memory and 60 megabytes of disk memory, a tape drive for backups, and its own emergency power supply.

We were the test site for an advanced computer system designed for congressional correspondence. And our system demonstrates what is happening and will be happening in offices and institutions across the country.

More and more people are learning to use computers as a routine part of their work. In my office, we do not have a single computer operator who would preside over this mysterious new technology like the priest of some powerful but unknowable force.

From the receptionist to the administrative assistant, the computer is a daily working tool in my Washington office. We have also connected our district offices with our in-house computer, so the Florida staff members are able to handle correspondence and casework through the computer. They direct the computer to produce letters, either from standard letters or directly from the keyboard, and these come out in Washington in the daily stream of the letters that makes up a substantial part of a congressional office's daily work. The computer system also handles messages and memoranda back and forth and allows us to create and modify documents in Washington or Florida.

My point is not to talk about computerized office procedures. Rather, I am trying to emphasize—perhaps a little like preaching to the convinced—to emphasize that familiarity with computers is becoming the common experience of tens of millions of working Americans. And where people work daily with a powerful tool such as a computer, there will be those who go far beyond normal day-to-day use to

overstep the boundaries between legitimate and criminal uses of these powerful devices.

It is estimated that there are more than 2 million computer operators, programmers, and technicians in the country. And I think this figure is far too low. It calculates primarily those who have a good deal of training in computer programming and operation, rather than the general use that is now becoming the norm for business and government offices.

Certainly the number of people familiar with computers outside of business and government is growing rapidly. It has been estimated that more than 6 million home computers are in use. This figure will explode in the next few years.

Moreover, these computers will increasingly be interfacing with the data banks of major institutions—banks, to direct the transfer of funds among the customers accounts; department stores, to order merchandise; TV polling operations, to get instant public reaction to public events, and many, many more.

So, granted that computers are becoming widespread in our society: Why should the Federal Government be involved? Why should theft and fraud and property damage be made Federal crimes when they involve computers?

Well, the Federal Government obviously has a direct interest when Federal agency computers are involved. The first electronic computer was designed for the military to calculate artillery trajectories in World War II. The first nonmilitary application—Univac I—was designed on contract for the Bureau of the Census. It cut the time for tabulating the 1950 census from more than 3 years to months—a remarkable achievement for the time. But Univac I was turned over to the Smithsonian as a museum piece in 1962. We have made considerable progress from those first vacuum-tube computers. With microchips, their capacity can virtually be held in your hand today.

The Defense Department has accepted the fact that computers are vulnerable to unauthorized penetration. Pentagon computers are compartmentalized so that a breach of security in one part will not enable an unauthorized person to access more than a small part of the total information in the system. Commercial computer systems have been developing similiar defenses against unauthorized users—along with programs to audit use to detect unauthorized use after it occurs.

It is also important that Government make its policy clear—that its computers and the computers systems vital to our national economy are not to be tampered with. This is one of the objectives of the legislation I am cosponsoring.

Federal legislation to strengthen the powers of Federal prosecutors to bring to justice those who illegally penetrate either the military or the civilian computers of the Federal Government obviously is in order.

Therefore, I urge passage of this legislation sponsored by my friend from New Jersey the chairman of the subcommittee. Enactment of this legislation into law will happily complete an 8-year effort to give U.S. attorneys a new Federal tool to prosecute this new type of criminal.

Mr. HUGHES. Mr. Speaker, will the gentleman yield to me?

Mr. NELSON of Florida. Certainly. I yield to the gentleman from New Jersey.

Mr. HUGHES. I thank the gentleman for yielding.

Mr. Speaker, I just want to thank the gentleman. Even though the gentleman is not a member of our Subcommittee on Crime, it was the gentleman from Florida who brought to my attention initially his great concerns over this area of criminal endeavor. I had not been sensitized to the extent of computer crime in this country because corporate America was very hesitant to come forward and tell just exactly what problems they had. They were embarrassed. They did not want to invite additional trespass on their data base. The gentleman from Florida worked extremely hard in the Florida Legislature in developing the model for many States around the country to follow in the area of computer crime.

□ 1245

I want to thank the gentleman for helping us lay the groundwork in the 98th Congress and working with us in this Congress to flush out the additional amendments that were needed to create an extraordinarily effective statute in my judgment. I want to thank the gentleman for that.

Mr. NELSON of Florida. The gentleman is very kind and I thank the gentleman for his leadership.

Mr. RODINO. Mr. Speaker, I rise in support of H.R. 4718, the Computer Fraud and Abuse Act of 1986. H.R. 4718 in general deals with what can be characterized as white collar crimes, which often are neglected both at the Federal and State levels. The prosecution of white collar crime, which silently robs millions of dollars from all of us, must remain in high priority for Federal law enforcement. It is in this perspective we must deal with computer fraud as we attempt to deter the theft of one of our most prized intangible commodities, information.

The Computer Fraud and Abuse Act of 1986 would accomplish this by setting up two new felonies, one involving any fradulent theft and the other malicious damage of $1,000 or more caused by unauthorized access to a Federal interest computer. The bill, therefore, covers computers used by the Federal Government or financial institutions, or conduct involving computers in different States. The bill also would proscribe trafficking in computer passwords as a misdemeanor offense. This latter conduct is associated with what is called pirate bulletin boards.

In passing this legislation, I believe the Congress will be providing needed and appropriate protection to our computer resources and, hopefully, decrease future attempts by high technology criminals in our society. A report by a task force on computer crime of the section of criminal justice of the American Bar Association stated:

The annual losses incurred as a result of computer crime appear, by any measure, to be enormous. Over 25% (72) of the survey respondents report "known and verifiable losses due to computer crime during the last twelve months." The total annual losses reported by these respondents fall somewhere between $145 million and $730 million. Thus, the annual losses per respondent reporting losses could be anywhere from $2 million to as high as $10 million. Approximately 28% of the survey respondents reported no available system to monitor or estimate the value of their computer crime losses.

Federal law must keep pace with technology. It is as important today to develop Federal protection for intangible property such as computerized information as it was to develop Federal law to protect tangible assets in interstate commerce in the past. I commend the chairman of the Subcommittee on Crime, Mr. HUGHES, and the ranking subcommittee member, Mr. MCCOLLUM, for their fine work on this legislation, and I urge my colleagues to support it.

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

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

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New Jersey [Mr. HUGHES] that the House suspend the rules and pass the bill, H.R. 4718, 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. HUGHES. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks, and to include extraneous matter, on H.R. 4718, the bill just passed.

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

There was no objection.

SENTENCING GUIDELINES ACT OF 1986

Mr. CONYERS. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4801) to amend section 994 of title 28, United States Code, to clarify certain duties of the U.S. Sentencing Commission, as amended.

The Clerk read as follows:

H.R. 4801

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 "Sentencing Guidelines Act of 1986".

SEC. 2. GUIDELINES AND POLICY STATEMENTS.

Section 994 of title 28, United States Code, is amended—

(1) in subsection (a)(2)—

(A) by redesignating subparagraphs (D) and (E) as subparagraphs (E) and (F), respectively;

(B) so that subparagraph (C) reads as follows:

"(C) the sentence modification provisions set forth in sections 3563(c), 3564, 3573, and 3582(c) of title 18;"; and

(C) by adding after subparagraph (C) the following: