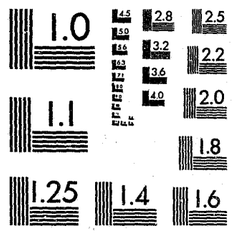

98204

98204

Department of Justice

STATEMENT

OF

JOHN C. KEENEY
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

SUBCOMMITTEE ON CRIME
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

CONCERNING

COMPUTER CRIME

ON

MAY 23, 1985

Mr. Chairman and Members of the Subcommittee, I am pleased to be here today to present the views of the Department of Justice on H.R. 1001 and H.R. 930, bills that would amend the new computer crime provision in the criminal code, section 1030 of title 18. Let me say, initially, that we greatly appreciate the Subcommittee's willingness once again to tackle this problem.

I should stress at the outset that the Administration fully shares the Subcommittee's concern about computer crime. In that regard, we expect to transmit to the Congress shortly the Administration's proposal in this important area. This legislative proposal which was described in the Administration's recent Management Report for 1986 will be an important part of our government-wide effort to improve management practices and crack down on fraud, waste, and abuse.

Before describing these two bills, I think it is important to review the steps that have been taken already in this difficult area, in large part due to the diligent efforts of this Subcommittee. As you know, Mr. Chairman, in the 98th Congress the House passed your bill dealing with computer crime, H.R. 5616, on July 24, 1984. Parts of this bill were included in the Comprehensive Crime Control Act which was signed by the President on October 12th of last year and those parts now make up section 1030.

Nevertheless, it is no secret that we felt H.R. 5616 contained a number of flaws which we pointed out while it was being considered last year. While we realize that this bill was drafted with the best of intentions, to date our experience with its provisions that are now in section 1030 have confirmed the view that this section is seriously defective. I will go over

these problems in a moment but suffice it to say that the provisions now in section 1030 simply are only of limited help to federal prosecutors around the country. Perhaps the Administration must shoulder some of the responsibility for this situation because we could not submit our alternative proposal in time for in depth consideration. In any event, because H.R. 1001 and H.R. 930 include several of the same problems as are in section 1030, I regret to state that the Department of Justice cannot support them.

Turning first to the provisions of H.R. 1001, this bill would amend 18 U.S.C. 1030 to provide for two new computer offenses. We note that these two offenses are identical to two provisions which were included in H.R. 5616 as that bill passed the House but were omitted from the portions enacted as part of the Comprehensive Crime Control Act of 1984. The first offense is a computer fraud offense. It would provide that whoever, having devised a scheme or artifice to defraud and with the intent to execute such a scheme or artifice, accesses a computer without authority (or, if the person has authority to access a computer for certain purposes, exceeds that authority by accessing the computer for purposes to which such authorization does not extend) and by means of such conduct obtains anything of value, other than the use of the computer itself, of $5,000 or more in any one-year period is guilty of an offense. This new crime would be a felony punishable by up to ten years' imprisonment and a fine of up to the greater of $10,000 or twice the value of the thing obtained for a first offense and carries even greater penalties for a subsequent conviction.

The second offense is described as an unauthorized access offense. It would make it unlawful to access a computer without

authority or in excess of one's authority and by means of such access to obtain anything of a value of $5,000 or more or to cause a loss of $5,000 or more. Because of technical amendments made to subsection 1030(a), a person who had authority to access a computer and exceeded his authority by accessing it for an unauthorized purpose would not be in violation of this provision if all the person did was to make unauthorized use of the computer. For example, a corporate employee who may legitimately access a computer owned by his company as part of his job but who used the computer to play video games or assist a child in a homework assignment would not violate the new provision. On the other hand, it would be a violation for a complete outsider to access the company computer by means of his home computer for such purposes if the person's access was of such duration as to be valued at $5,000 and if this could be proven. This new offense would be a misdemeanor punishable by up to a year's imprisonment and a fine extending to the greater of $5,000 or twice the value of the property obtained or the loss created, although a second conviction of this offense would be punishable as a felony with up to ten years' imprisonment and an enhanced fine.

As for the computer fraud offense, our most basic objection is that it does not track the language of the existing mail and wire fraud statutes so that the extensive body of law that has been developed interpreting these provisions can be applied to computer fraud. In our view, the focus of the offense should be the devising of a scheme or artifice to defraud, or to obtain money or property by false or fraudulent pretenses, or to embezzle, steal, or convert the property of another if, for the

purpose of carrying out the offense, the defendant accesses or attempts to access a computer with a particular federal nexus. A computer is thus the vehicle -- comparable to the mails or interstate telephone wires -- through which the fraud or other crime is committed. The way the proposed paragraph 1030(a)(4) is drafted in H.R. 1001 would require the government to prove that the offense affected interstate or foreign commerce and resulted in a $5,000 gain or loss. Proving that a particular scheme actually affected interstate commerce diverts the attention of the jury from what should be the central issue in the case, namely did the defendant devise a fraud scheme and, if he did, for the purposes of carrying it out, did he access a particular type of computer. Requiring a jury finding of an effect on interstate commerce invites all sorts of defense tactics designed to downplay the fraud scheme's effect on commerce and to get the jury to focus on this rather than on the gist of the defendant's scheme. Moreover, limiting the offense to situations in which the person has caused a loss or realized a gain of at least $5,000 is unnecessarily restrictive and can cause enormous practical problems. If, for example, a dishonest bank employee managed, by means of manipulating the bank's central computer, to divert a very small amount of money such as two or three cents a month from hundreds of individual accounts into one which he controlled, he would obtain a sizeable sum over a period of time. But the new provision would be of no avail if he did not obtain $5,000 in any one year.

Still another major objection to this method of drafting a computer fraud offense stems from the fact that it would require the government to prove the extent of the defendant's authority to access the computer used in the crime. Requiring proof of lack of authority makes no sense in cases involving the use of a computer to defraud. The offense is the economic crime of illegally diverting money or property. Use of a particular computer should be merely the factor that establishes federal jurisdiction. Whether the person lacked authority to access the computer at all or exceeded his authority by accessing it as part of an unlawful scheme should make no difference and there is no justification for making the government prove it. Requiring proof of such an element merely gives the defendant a chance to raise an issue that is in no way related to his criminal conduct.

Turning to the unauthorized access offense, this offense is also much too limited by the requirement that the access result in the gain or loss of $5,000, and the minimal protection it does offer is given to the wrong types of computers. In our view, what is needed is a misdemeanor covering the unauthorized access of certain computers in which there is a strong federal interest -- those owned by or operated on behalf of the government of the United States and federally insured financial institutions -- without proof of the obtaining of anything of value such as information or the time of the computer itself. Such conduct is akin to a deliberate trespass onto another person's property or a surreptitious entry to rummage through desks and file cabinets in the hopes of picking up something useful or interesting and

carries the potential for serious harm. Yet this provision in H.R. 1001 would only cover unauthorized access to a computer if it could be shown to affect interstate commerce and to result in a gain or loss of at least $5,000. As I have indicated, proving that a particular computer access affected interstate commerce may be difficult and unnecessarily confusing to the jury. In addition, if the thing obtained is information, proving value is often very difficult. Similarly, proving the value of computer time could be difficult, although we recognize that such proof is not impossible in many situations.

We realize that the reason this unauthorized access provision does not cover computers operated for or on behalf of the federal government is that an offense of this nature is already set out in subsection 1030(a)(3). However, subsection 1030(a)(3) is not a true unauthorized access offense because it requires the using, modifying, destroying, or disclosing of the information or preventing authorized use of the computer. Moreover, this provision contains the requirement that the unauthorized access to the computer and the use or destruction of the information therein is a crime only "if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation." Grammatically, it would seem that this should be read to require the government to prove that the person's conduct affected the operation of the computer. However, the legislative history of this provision as it was originally set out in H.R. 5616 indicates that the prosecutor must prove that the unauthorized access and use or destruction of the

the information affect the operation of the government. 1/ That will usually be a very difficult element to prove since unauthorized access to a computer of the government will likely have only a de minimis effect on even the agency involved. Even if it were clearly spelled out that such a de minimis effect is all that is required the presence of this element -- like the requirement that the computer fraud offense affect interstate commerce -- can serve only to divert the jury's attention from the critical point which is whether the defendant committed a trespassory type of offense against government records and information. In our view, a crime is committed every time such a trespass takes place and no more proof should be required than that the trespass occurred.

H.R. 930. H.R. 930 would also amend section 1030 of title 18 by adding a new subsection (f) which would proscribe accessing certain computers without authority or in excess of one's authority and thereby obtaining property of another or modifying or destroying property of another. The term property is defined very broadly to include information, services, and data processing and storage functions. Thus virtually any unauthorized access to a covered computer that resulted in the obtaining of information or altering or destroying information stored in the computer would be a violation of this new subsection. I would note initially that this unauthorized access provision is an

---

1/ House Report No. 98-894, The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, July 24, 1984, p. 22.

improvement over that set out in H.R. 1001 in that it does not require that the government prove that the information taken, modified, or destroyed has any particular value. It does require, however, that it have some value and that it be taken, modified, or destroyed and so, like the offense in H.R. 1001, is not a true unauthorized access offense. This is significant because there are certain situations where the government should not be required to prove that information obtained or altered had any value or even that information was indeed obtained or altered. For example, a law enforcement agency that has been compiling information on widespread criminal activity by a major corporation in preparation for a grand jury investigation obviously wants none of the information to be revealed prematurely and a person who accesses this information without authority is acting reprehensibly. Proving that the person who without authority merely scans through the information in the government computer out of idle curiosity has actually "obtained" any information may be difficult and even if this hurdle can be overcome proving that the information obtained had some value would likely be more of a problem. Yet the government has, in our view, just as much of an interest in punishing the idle perusing of such information by the curious and technically proficient "hacker" as it does in preventing a merely curious and athletically inclined person from successfully negotiating several security fences just to look around a secret area on a military base.

An even more serious problem with this provision, though, is the fact that the new subsection (f) does not cover the unauthorized access to the right types of computers, in our view. It covers unauthorized access to computers owned or operated by or under contract to a federally insured financial institution or computers operating in or using a facility of interstate commerce. However, it does not cover unauthorized access to computers owned by or operated on behalf of the government of the United States, the very computers in which the federal government has the greatest interest in protecting. Obviously, again, this is because such conduct is already at least partially covered in subsection 1030(a)(3) but as I have indicated this provision is inadequate and itself should be modified. The coverage of financial institution computers is a step in the right direction, but the further coverage of any computer operating in or using a facility of interstate commerce may well go too far. Conceptually, we are not opposed to such an offense, but we think it would be preferable to limit, at least at first, a federal unauthorized access offense to computers in which there is a strong federal interest, namely the government's own computers and those of federally insured financial institutions.

Mr. Chairman, so far I have tried to set out why, in our view, the present unauthorized access offense (18 U.S.C. 1030(a)(3)) is inadequate and why the provisions in both H.R. 1001 and H.R. 930 fail in their attempts to make needed improvements. I have also pointed out why the computer fraud offense in H.R. 1001 should be drafted differently. The

Administration's bill submitted in the 98th Congress and which will be submitted again in the near future sets out what we think are far more effective computer fraud and unauthorized access provisions. Before describing these provisions in more detail, let me just go over what we think are some of the problems with the other two parts of subsection 1030(a) which would be largely overcome by the Administration's bill.

Subsection 1030(a)(1) proscribes the use of a computer without authority or in excess of one's authority to obtain classified information or restricted data relating to national defense, foreign relations, or the Atomic Energy Act of 1954. The offense is a felony, as indeed it should be, but it is largely redundant and unnecessary because other statutes proscribe the unauthorized possession or retention of the same information and provide for the same or harsher penalties. 2/

Subsection 1030(a)(2) proscribes using a computer without authority or in excess of one's authority to obtain information contained in a financial record covered by the Right to Financial Privacy Act or in a file of a consumer reporting agency on a consumer as defined in the Fair Credit Reporting Act. This offense is a misdemeanor although a second conviction under this provision would be a felony. This provision at least sets out an offense not covered by existing federal statutes but it is unjustifiable to single out only a very limited class of

---

2/ 18 U.S.C. 793, 794; 42 U.S.C. 2275; 50 U.S.C. 783

financial and credit information for protection against unauthorized computer access. For example, it would prohibit such unauthorized access to a bank's computer to obtain information contained in the account of an individual or a partnership of five or fewer persons, but would give no protection to corporate accounts or the bank's own records of its deposits in other institutions and loans. It would prohibit obtaining credit information on an individual but not on even the smallest of corporations. Moreover, it is not apparent why the offense should be limited to unauthorized computer access to personal financial records. If the idea is to add extra protection for information concerning individuals which most persons would agree should enjoy a high degree of confidentiality, then probably many other types of information, such as tax return information and census data should also be covered.

In short, we think that the present provisions in 18 U.S.C. 1030 need to be replaced in their entirety, not supplemented with the kinds of provisions that are in H.R. 1001 and H.R. 930. What we would suggest is a felony computer fraud provision that deliberately tracks the mail and wire fraud provisions for the reasons that I have already discussed. We think federal jurisdiction should extend to such an offense if the computer is owned by, under contract to, or operated on behalf of the federal government or a federally insured financial institution or when two or more computers are used which are located in different states.

Second, we think that it should be a federal felony to knowingly and willfully destroy any computer owned by, under contract to, or operated on behalf of the federal government or a federally insured financial institution, or a computer program or data contained in such a computer.

Third, we think it should be a misdemeanor to intentionally and without authorization access a computer owned by, under contract to, or operated on behalf of the federal government or a federally insured financial institution. This provision should be drafted in such a way that it could be proven without showing that any information was obtained or used. As I have indicated, the offense is basically a trespass and proof of mere intentional unauthorized access should be all that is required.

Finally, we recommend that legislation in this area contain a criminal forfeiture provision under which the defendant's interest in any computer or computer software involved in any of the above offenses could be forfeited to the government on his conviction. Such a provision would be an especially effective deterrent for persons who use their home or small business computer to make unauthorized access to a government computer. Courts are unlikely to give prison sentences or meaningful fines to such persons, and the unauthorized access offense is proposed as only a misdemeanor in any event, but the prospect of losing their expensive computer could act as a powerful deterrent and serve as a uniquely appropriate punishment for this type of activity. Moreover, a person who has developed and sold computer software knowing that it facilitates a fraud scheme or

unauthorized access to a computer network by others should be made to forfeit his interest in the software. For the information of the Subcommittee, I am attaching a copy of the Administration's bill on computer crime, S. 2940, introduced in the last Congress. It contains language precisely setting out the above concepts.

Mr. Chairman, again let me say that I regret the Department cannot support either bill before the Subcommittee today. We are not unappreciative of your efforts in this area, but as you know, this is a very difficult subject and therefore the Department feels constrained to recommend a fresh start.

That concludes my statement and I would be pleased to answer any questions.

98TH CONGRESS
2D SESSION

S. 2940

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and other computers where the offense involves interstate or foreign commerce.

IN THE SENATE OF THE UNITED STATES

AUGUST 9, (legislative day, AUGUST 6), 1984

Mr. THURMOND (by request) introduced the following bill; which was read twice and referred to the Committee on the Judiciary.

A BILL

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and other computers where the offense involves interstate or foreign commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Computer Systems Protection Act of 1984".

SEC. 2. (a) Chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following new section:

"§ 1028. Computer fraud and abuse

"(a) Whoever having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by false or fraudulent pretenses, representations, or promises, or to embezzle, steal, or convert to his use or the use of another, property not his own, for the purpose of executing such scheme or artifice or embezzlement, theft, or conversion, or attempting to do so, knowingly accesses or attempts to access a computer, shall—

"(1) if the computer is owned by, under contract to, or operated for or on behalf of—

"(A) the United States Government; or

"(B) a financial institution; or

"(2) if in committing or concealing the offense two or more computers are used which are located in different States or in a State and a foreign country;

be fined not more than two times the amount of the gain directly or indirectly derived from the offense or $50,000, whichever is higher, or imprisoned not more than five years, or both.

"(b) Whoever knowingly and willfully without authorization damages, destroys, or attempts to damage or destroy a computer described in subsection (a) (1) and (2) or knowingly and willfully without authorization damages or attempts to damage any computer program, or data contained in such

computer shall be fined not more than $50,000 or imprisoned not more than five years, or both.

"(c) Whoever intentionally and without authorization accesses a computer as defined in (a)(1), or a computer system or computer network including such computer, shall be guilty of a misdemeanor and shall be fined not more than $25,000 or imprisoned for not more than one year, or both.

"(d) Whoever violates any provision of paragraph (a), (b), or (c) shall forfeit to the United States any interest acquired or maintained in any computer and computer software, which has been used to commit the violation. Upon conviction under this section, the court shall authorize the Attorney General to seize all property or other interest declared forfeited under this section upon such terms and conditions as the court shall deem proper. If a property right or other interest is not exercisable or transferable for value by the United States, it shall expire, and shall not revert to the convicted violator. The United States shall dispose of all such property as soon as commercially feasible, making due provision for the rights of innocent persons.

"(e) The Attorney General is authorized to delegate, in whole or in part, to other departments and agencies concurrent investigative authority under this section subject to agreement between the Attorney General and the department or agency affected.

"(f) DEFINITIONS.—For the purpose of this section the term—

"(1) 'computer' means an electronic, magnetic, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device;

"(2) 'computer system' means a set of related connected or unconnected computers, computer equipment, devices, and software;

"(3) 'computer network' means two or more interconnected computers, computer terminals, or computer systems;

"(4) '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 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) a member or business insured by the Securities Investor Protection Corporation; and

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

"(5) 'property' includes, but is not limited to, financial instruments, information, including electronically processed or produced data, and computer program and computer software in either machine or human readable form, computer services, and any other tangible or intangible item of value;

"(6) 'financial instrument' means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card or marketable security, or any electronic data processing representation thereof;

"(7) 'computer program' means an instruction or statement or a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system;

"(8) 'computer software' means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system;

"(9) 'computer services' includes but is not limited to computer time, data processing, and storage functions;

"(10) 'United States Government' includes a branch or agency thereof; and

"(11) 'access' means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network."

SEC. 3. The table of sections of chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following:

"1028. Computer fraud and abuse.".

O

DOJ-1985-05

END