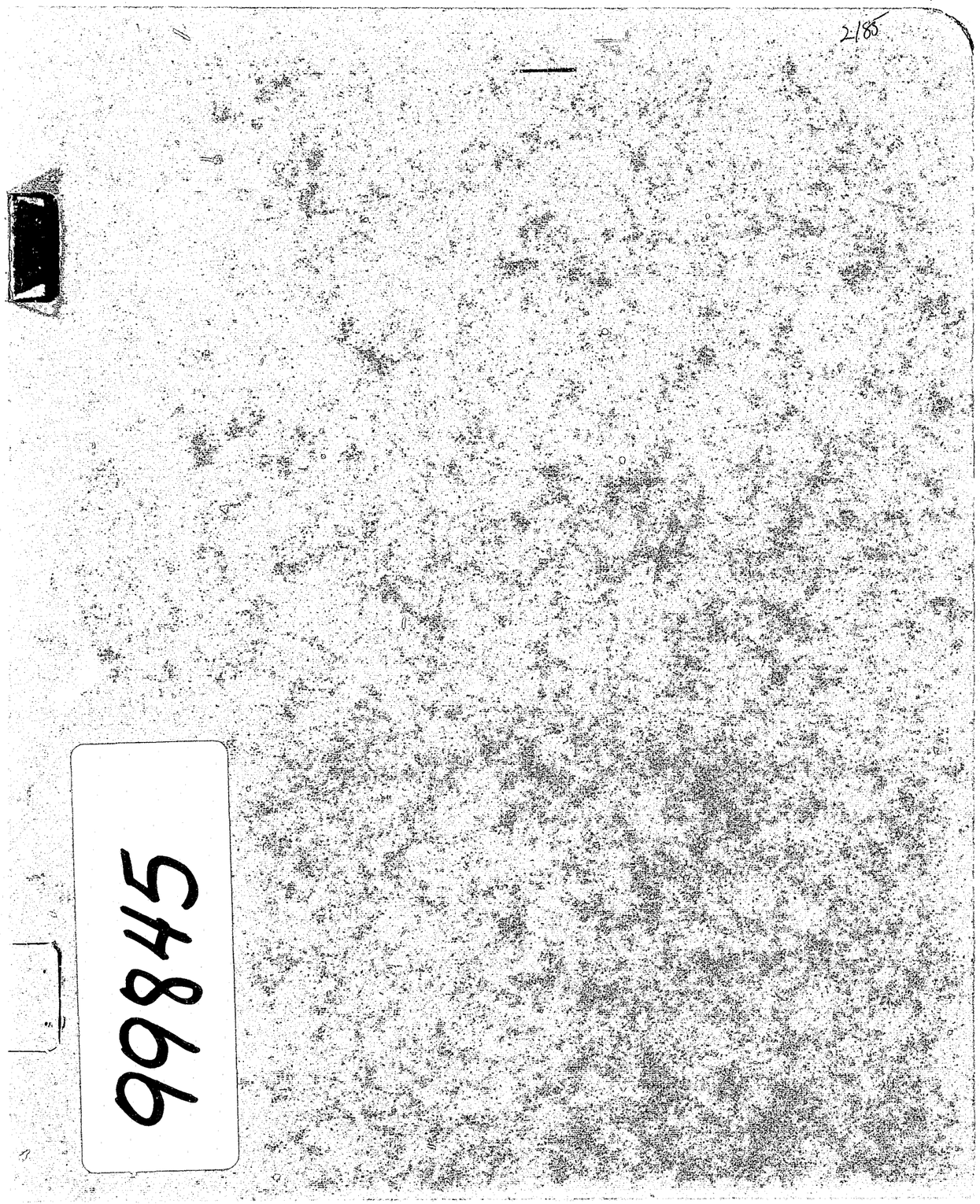

Department of Justice

VICTORIA TOENSING
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIMINAL LAW
UNITED STATES SENATE

CONCERNING

COMPUTER CRIME LEGISLATION

ON

OCTOBER 30, 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 Computer Crime legislation. The potential for the use of computers in a variety of criminal schemes has been well documented. The Congress dealt with this sometimes complex subject in the Comprehensive Crime Control Act of 1984 and the result is a new section of the criminal code, 18 U.S.C. 1030, which proscribes certain computer related offenses.

Nevertheless, section 1030 in its present form is inadequate and revisions must be made for a really effective federal computer crime statute. In this regard, the Administration has prepared a computer crime bill, S. 1678, that would substantially improve the federal computer crime statute. This proposal is part of the President's comprehensive management reform legislation initiative, which he announced on July 31, 1985. Let me first outline the existing provisions in section 1030 and describe some of their shortcomings. Then I will explain why the concepts contained in the Administration's computer crime proposal merit serious and favorable consideration.

18 U.S.C. 1030 sets out three distinct computer-related offenses. 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. Clearly, the unauthorized obtaining of this type of data is a serious matter and deserves to be punished as a felony. That much of these data are stored in computers has made them much more

vulnerable to unauthorized disclosure than they were a generation ago. Nevertheless, the offense in subsection (a)(1) 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, regardless of whether or not a computer is used. 1/ In short, subsection 1030(a)(1), while not harmful, is simply not very helpful to federal prosecutors. It is quite hard to imagine a case in which it would be easier to use this provision in prosecuting a criminal case than one of the older offenses that prohibit unauthorized access to important national security information.

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" of a "financial institution," as those terms are defined in the Right to Financial Privacy Act of 1978, 2/ or to obtain information in a file of a "consumer reporting agency" on a "consumer," as those terms are defined in the Fair Credit Reporting Act. 3/ This offense is a misdemeanor, although a second conviction under this subsection would be treated as a felony. We certainly agree that this type of extremely revealing information about a person's financial affairs should not be disclosed without authorization. The fact

---

1/ 18 U.S.C. 793, 794; 42 U.S.C. 2275; 50 U.S.C. 783.

2/ 12 U.S.C. 3401 et seq.

3/ 15 U.S.C. 1681 et seq.

that a lot of it is stored in computers has undoubtedly made it more vulnerable to such disclosure. For that reason, subsection 1030(a)(2) may be of some limited utility.

It is unjustifiable, however, to single out only a very limited class of financial and credit information for protection against unauthorized computer access. For example, 1030(a)(2) prohibits 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 to the bank's own records of its deposits in other institutions and loans because these are not within the purview of the Right to Financial Privacy Act. The subsection would, for similar reasons involving the scope of the Fair Credit Reporting Act, prohibit the unauthorized obtaining of credit information on an individual but not on even the smallest of corporations. Simply put, it makes no sense to restrict this offense to unauthorized computer access to personal financial records. If the objective of subsection (a)(2) is to protect against the use of computers to obtain certain personal information concerning individuals which enjoys, through operation of other federal laws, a high degree of confidentiality -- a laudable goal -- the use of computers to obtain many other types of personal information (such as tax return information and census data) should also be covered.

Subsection 1030(a)(3) proscribes using a computer without authority or in excess of one's authority, and by means of such conduct using, modifying, destroying, or disclosing information

in the computer or preventing authorized use of the computer "if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation." This offense also is a misdemeanor, but a second conviction would be punished as a felony. We certainly agree that unauthorized access to the computers of the federal government should be a crime. Subsection (a)(3) is inadequate because it is not a true unauthorized access offense. Instead, it requires the using, modifying, destroying or disclosing of the information or preventing authorized use of the computer. As I will explain in more detail shortly when I outline the Administration's bill, we think the unauthorized access offense, particularly with respect to the federal government's computers, is most like a physical trespass onto government property or into a government building and should be punishable without a showing that the person made any use of or destroyed any information, or that he or she prevented any other person from gaining access to the computer.

Moreover, as I indicated, subsection 1030(a)(3) contains a jurisdictional element that could limit its usefulness even further. The proscribed conduct is a federal crime only if the computer involved "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 indicates that the prosecutor must prove that the unauthorized access to and use or destruction of the information

in the computer affected the operation of the government. 4/ That will usually be a very difficult element to prove since unauthorized access to a government computer will likely have only a de minimis effect on even the agency involved. Even if it were clearly spelled out that such a trivial effect is all that is required, the presence of this element can only serve to divert the jury's attention from the crucial question at issue which is whether the defendant committed a trespassory type offense against government records and information. In our view, every such trespass should be considered a crime without proof of how seriously the intrusion affected the government.

At this point, Mr. Chairman, I think it would be helpful for me to set out some concepts that the Administration believes should be included in any revision of the computer crime provisions in section 1030. Each of the concepts is incorporated in our computer crime bill, S. 1678. First, as I have just discussed, it should be an offense to willfully obtain unauthorized access to a computer owned by or operated on behalf of the United States, without a showing that any information was obtained or that the unauthorized access prevented someone else from

---

4/ This provision was originally included in H.R. 5616 which passed the House on July 24, 1984. The parts of this bill that are now 18 U.S.C. 1030 were then included as a last minute amendment to the Comprehensive Crime Control Act, the legislative history of which makes no mention of the computer crime provision. For a brief discussion of the provision in H.R. 5616 which became 18 U.S.C. 1030(a)(3) see House Report No. 98-894, 98th Cong., 2d Sess., July 24, 1984, p. 22.

in the computer or preventing authorized use of the computer "if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation." This offense also is a misdemeanor, but a second conviction would be punished as a felony. We certainly agree that unauthorized access to the computers of the federal government should be a crime. Subsection (a)(3) is inadequate because it is not a true unauthorized access offense. Instead, it requires the using, modifying, destroying or disclosing of the information or preventing authorized use of the computer. As I will explain in more detail shortly when I outline the Administration's bill, we think the unauthorized access offense, particularly with respect to the federal government's computers, is most like a physical trespass onto government property or into a government building and should be punishable without a showing that the person made any use of or destroyed any information, or that he or she prevented any other person from gaining access to the computer.

Moreover, as I indicated, subsection 1030(a)(3) contains a jurisdictional element that could limit its usefulness even further. The proscribed conduct is a federal crime only if the computer involved "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 indicates that the prosecutor must prove that the unauthorized access to and use or destruction of the information

in the computer affected the operation of the government. 4/ That will usually be a very difficult element to prove since unauthorized access to a government computer will likely have only a de minimis effect on even the agency involved. Even if it were clearly spelled out that such a trivial effect is all that is required, the presence of this element can only serve to divert the jury's attention from the crucial question at issue which is whether the defendant committed a trespassory type offense against government records and information. In our view, every such trespass should be considered a crime without proof of how seriously the intrusion affected the government.

At this point, Mr. Chairman, I think it would be helpful for me to set out some concepts that the Administration believes should be included in any revision of the computer crime provisions in section 1030. Each of the concepts is incorporated in our computer crime bill, S. 1678. First, as I have just discussed, it should be an offense to willfully obtain unauthorized access to a computer owned by or operated on behalf of the United States, without a showing that any information was obtained or that the unauthorized access prevented someone else from

---

4/ This provision was originally included in H.R. 5616 which passed the House on July 24, 1984. The parts of this bill that are now 18 U.S.C. 1030 were then included as a last minute amendment to the Comprehensive Crime Control Act, the legislative history of which makes no mention of the computer crime provision. For a brief discussion of the provision in H.R. 5616 which became 18 U.S.C. 1030(a)(3) see House Report No. 98-894, 98th Cong., 2d Sess., July 24, 1984, p. 22.

legitimately accessing the computer. Clearly, protecting the federal government's own computers is an altogether proper matter for federal jurisdiction. While we realize that many states now have computer crime provisions and that in theory these statutes could be applied to offenses against federal computers, it is not realistic to expect the states to take on this responsibility.

Unauthorized access to a computer owned by or operated on behalf of a federally insured financial institution should also be a federal offense. There is a very clear federal interest in protecting these institutions such as banks, savings and loans, and brokerage firms against computer crimes.

Second, we believe there should be a computer fraud offense. One of the most important reasons for having any federal computer offense is that computers may allow an old fashioned crime like theft or embezzlement to be committed in such a way that existing federal statutes do not cover it. As you know, federal jurisdiction over offenses of this type is grounded on such factors as the Commerce Clause, which justifies the federal mail and wire fraud statutes (18 U.S.C. 1341 and 1343) and federal regulation and insurance of many types of financial institutions which justifies such offenses as the new bank fraud statute (18 U.S.C. 1344), and the theft and embezzlement offense set out in 18 U.S.C. 656.

There is, however, a potential problem with the use of fraud or theft statutes, since these statutes antedate the invention and widespread use of computers. I stress that this is a

potential problem because so far at least we have been able to prosecute computer fraud cases under existing statutes. For example, in a case in which a person made telephone access approximately fifty times to the computer system of a previous employer to steal confidential software, two of the calls were made across state lines which brought into play the wire fraud statute. In another case, a former employee of the Federal Reserve Board gained access to information in the Board's file that kept track of money supply information that would have been very useful to clients in his new job as a private financial analyst. Fortunately, the defendant in that case eventually pled guilty to a violation of 18 U.S.C. 1001, in essence admitting that his making an unauthorized access to the Federal Reserve Board's computer constituted a "false statement." If he had not pleaded, proving a violation of 18 U.S.C. 1001 under these facts would have been difficult, and prosecuting the defendant for theft of government property would have been problematical because proving the value of the information about the money supply, a necessary element of proof, also would have been arduous.

In the future we may not be so fortunate. Consequently, there should be enacted a specific offense, as contained in our bill, modeled on the mail and wire fraud statutes, of devising 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 a computer with a particular federal nexus. The computer is thus the vehicle -- comparable to

the mails or interstate telephone wires -- through which the fraud offense is committed.

Under our proposal, federal jurisdiction would attach to the computer fraud offense in cases in which the computer involved is owned by or operated on behalf of the federal government or a federally insured financial institution, or if the offense involves computers located in two or more states or in a state and a foreign country. This two-state provision (which is far less of an assertion of federal jurisdiction than would be a provision to extend jurisdiction over a fraud scheme involving any computer operating in or affecting interstate commerce) would reserve federal jurisdiction for those cases where it is most needed and for those which the states are the least capable of investigating and prosecuting. For example, a state's laws only apply within its borders and it is unrealistic to expect a state to undertake the investigation and prosecution of a fraud scheme that made use of computers in several different states, even if its laws were deemed applicable to some of the criminal conduct.

The Administration's proposal tracks the language of the mail and wire fraud statutes as much as possible so that the extensive body of case law that has been developed with respect to these statutes can be applied. In this regard, I would emphasize that we oppose a provision in the computer fraud offense that was passed by the House in the last Congress. That provision would have required the government to prove that the defendant lacked authority to access the computer involved in the crime. Requiring proof of lack of authority makes no sense in

cases which involve the use of a computer to divert illegally money or other property. While proof of lack of authority may make considerable sense if the offense is designed to protect privacy interests, computer fraud should be regarded as an economic crime designed to protect property interests, and access authority or the lack thereof is not relevant.

Third, our bill would make it a federal crime, punishable as a felony, to destroy willfully and without authority any computer owned or operated on behalf of the federal government or of a federally insured financial institution, or a computer program or data contained in such a computer. There is a clear federal interest in protecting this limited class of computers from physical destruction and from having the data they contain erased or altered. Such a provision would represent only a very minimal expansion of federal jurisdiction into an area traditionally reserved for the states.

Finally, any new computer crime legislation should contain a criminal forfeiture provision under which the defendant's interest in any computer involved in the unauthorized access offense, the computer fraud offense, or the computer destruction offense could be forfeited to the government on his conviction. Such a provision might prove to be an especially effective deterrent for persons who would use their home or small business computer to make unauthorized access to a government computer. Historically, courts have not given prison sentences or meaningful fines to such persons. In any event, the unauthorized access offense should properly be a misdemeanor. Nevertheless,

the prospect of losing an expensive computer could act as a powerful deterrent and serve as a uniquely appropriate punishment for this type of offense.

Mr. Chairman, as I indicated previously, all of the above suggestions are contained in S. 1678, a bill drafted by the Department which Chairman Thurmond introduced and which you co-sponsored. That bill would repeal the provisions in the present section 1030 of title 18 and would make a fresh start in this difficult area. That is the approach we favor but we realize the Subcommittee may decide merely to amend section 1030. If the Subcommittee decides on this approach, I hope that as many of our suggestions as possible will be included. 5/

Mr. Chairman, that concludes my prepared statement and I would be happy to answer any questions at this time.

5/ Another matter that should be included in any revision of section 1030 is a provision stating that nothing in the section is intended to prohibit any duly authorized investigative, protective, or intelligence activity of a state or federal law enforcement agency or of an intelligence agency of the United States. Such a provision is in both S. 1678 and S. 1236, the Department's bill making technical amendments to the Comprehensive Crime Control Act of 1984. A similar exemption was included in 18 U.S.C. 1029, regarding credit card fraud, and also enacted as part of the Comprehensive Crime Control Act. Originally, sections 1029 and 1030 were part of the same House bill and the law enforcement and intelligence exemption, intended to apply to both sections, was inadvertently dropped from the computer crime provision when parts of that bill were added to the Comprehensive Crime Control Act by the House and Senate conference.

END