DOCUMENT RESUME

06293 - [B1746790]

Federal Computer Systems Protection Act of 1978 (S. 1766). June 22, 1978. 12 pp.

Testimony before the Senate Committee on the Judiciary: Criminal Laws and Procedures Subcommittee; by D. L. Scantlebury, Director, Financial and General Management Studies Div.

Contact: Financial and General Management Studies Div.
Congressional Relevance: Senate Committee on the Judiciary: Criminal Laws and Procedures Subcommittee.
Authority: Federal Computer Systems Protection Act of 1978; S. 1766 (95th Cong.).

The growing use of computers in Government operations has made computer crime a serious problem resulting in losses in money, equipment, and data, and in personnel injuries. Computer crimes against the Government include fraudulent input, unauthorized use of computer-related facilities, destruction or alteration of data and computer hardware and software, and thefts of Government property. About 62% of the crimes involved fraudulent input. Internal controls over data processed through computer systems have been inadequate. Millions of actions take place on automated systems without manual checks. Action is being taken to improve controls, including issuance of policy guidance by central management agencies and strengthening controls at some agencies. Strong deterrents in the form of punishment, such as provided for in S. 1766, are important means for protection against computer fraud and abuse. (HTW)

6790

UNITED STATES GENERAL ACCOUNTING OFFICE
Washington, D.C. 20548

FOR RELEASE ON DELIVERY
Expected at 10:00 a.m. EST
Thursday, June 22, 1978

STATEMENT OF

Donald L. Scantlebury
Director

Financial and General Management Studies Division

Prepared for the

SUBCOMMITTEE ON CRIMINAL LAWS & PROCEDURES
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
on the
FEDERAL COMPUTER SYSTEMS PROTECTION
ACT OF 1978 (S-1766)

Mr. Chairman and Members of the Subcommittee:

We welcome this opportunity to appear before your Subcommittee to discuss the issue of computer-related crime and fraud, for we in GAO have been concerned for some time about the need for more protection against the many types of crimes that affect computer systems. Before proceeding I would like to introduce, Mr. Walter Anderson, Associate Director, of the Financial and General Management Studies Division, who is accompanying me today.

The use of computers has become widespread in the past few years. So much so that they are now indispensible to the delivery of Government services, with virtually all Government agencies dependent upon computers for carrying out programs and missions. Today, there are nearly 12,000 computers in the Government's inventory and there is every indication that the number will increase. These computer systems impact almost every aspect of Government operations, and have changed the way in which functions are performed and transactions carried out. Moreover, the computer has made obsolete many traditional methods of control, and has created a need for improved methods to assure the protection of the Government's funds and other assets.

In the past couple of years GAO reviews have shown that computer crimes are a serious problem in the Federal Government. The computer crimes we reviewed have resulted in:

--Sizeable dollar losses;

--Damages to building and equipment;

--Losses of software and data;

--Personnel injuries; and, in one case

--A loss of life.

The types of crimes that produced these results parallel those cited in the bill. They include:

--Fraudulent input into the systems.

--Unauthorized use of computer-related facilities.

--Destruction or alteration of data and computer hardware and software.

--Thefts of Government property, including cash, valuable data, and other assets.

Let me cite some information from two of our reports:

- --Computer-Related Crimes in Federal Programs (FGMSD-76-27, April 27, 1976).
- --Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities (FGMSD-76-40, May 10, 1976).

FRAUDULENT INPUT

Our studies show that the majority of computer crimes against the Federal Government--about 62 percent--involved persons preparing fraudulent input to computer-based systems.

We found many cases in which fraudulent input data was introduced into systems that make direct payments to individuals or businesses. The results were fraudulent payroll, social welfare, and compensation payments as well as payments for nonexistent goods and services. For example, a supervisory clerk responsible for entering claim transactions to a computer-based social welfare system found that she could introduce fictitious claims on behalf of accomplices and they would receive the benefits. She was was able to process over $90,000 in known fictitious claims (authorities believe such claims might have totaled as much as $250,000) before she was discovered.

Other cases involved individuals stealing Government property through the use of computers. For example, a perpetrator used a computer terminal to ascertain the

the location and availability of items desired by outside conspirators. Once he located those items, the perpetrator caused the system to prepare fraudulent requisitioning documents. Then he used the documents to obtain the items he wanted, took the items from the installation, and sold them to the outside parties.

The total amount of property stolen through computerized supply systems cannot easily be determined, but our review revealed a number of such cases. One loss of over $300,000 was averted when discrepancies were discovered and the material recovered.

UNAUTHORIZED USE OF FACILITIES

Another type of crime, which has occurred in several agencies, is the unauthorized use of computers by ADP personnel. An engineer who was no longer employed at one Government installation managed to continue using the equipment for his own purposes. Before he was discovered, he had used over $4,000 worth of computer time. At another installation, a programer used a self-initiated training program to obtain use of his agency's computer system. But instead of working on the training exercise, he was developing his own computer programs which he hoped to sell.

Computer-related crime does not always lead to direct losses of Government funds or property. In one case we reviewed, the manager of a non-Federal computer center processing personal information for the Government, was able to steal some of this data and sell it to outside parties who were not authorized to use it. Although the Government did not lose any money, the privacy of individuals whose data records were involved was violated, and this is of concern in protecting the privacy of personal information.

DESTRUCTION OR ALTERATION OF COMPUTER HARDWARE, SOFTWARE AND VALUABLE DATA

We also found a number of cases involving losses of computer facilities or data.

On August 24, 1970, a bomb exploded outside the Sterling Hall Building at the University of Wisconsin. This building housed the Army Mathematics Research Center and other federally funded research activities. One employee was killed and three others were injured during this incident. This explosion damaged 25 buildings at the university, and resulted in a total loss of about $2.4 million for buildings and equipment. Computers at the Army Mathematics Research Center were damaged, and some programing efforts and 20 years' accumulated data was destroyed. It has been estimated that this research data represented over 1.3 million staff hours of effort which we calculate to represent an investment of about $16 million. The intent of the persons who did the bombing is not known to us but it seems likely to us that the target was the computer facility.

Attempts at sabotage of computers have also been made by employees within data processing centers. For example, there were four attempts to sabotage computer operations at Wright-Patterson Air Force Base during a 6-month period, by using magnets, loosening wires on the computer mainframe, and gouging equipment with a sharp tool.

During our study we identified other locations which were susceptible to sabotage. For instance, in some cases outside personnel were not carefully monitored while on the premises or in the computer areas.

We have even heard of cases in which disgrunted persons shot or used other tools to attack and damage computer equipment.

THEFT OF GOVERNMENT PROPERTY

Computerized systems are also vulnerable to theft or stealing by electronic means or otherwise. We noted numerous cases of publicized thefts or misuses involving

--data or assets,

--financial frauds,

--embezzlements, and

--mistakes made by computer employees.

Industry literature indicates thefts or misuses of computer systems are increasing at an alarming rate.

One case we noted during our study involved theft of Government funds at Kelly Air Force Base, San Antonio, Texas. The Government paid approximately $100,000 to bogus fuel companies for aircraft fuel never delivered to the Air Force. The bogus fuel companies were established by a dishonest Government employee working at the air base. This employee had indepth knowledge of the computerized fuel accounting system which he helped develop and install. An investigation of this matter was initiated when a bank contacted the Air Force regarding suspicious banking transactions involving Government checks. The employee was later arrested.

Other studies of theft and misuse to data processing operations have been identified within the Federal Government and private sectors. Noteworthy were March 1973 studies by the Stanford Research Institute on "Threats to

Computer Systems" and a November 1973 study on "Computer Abuse." Each study catalogued over 100 data processing security incidents within and outside the Federal Government that were identified from sundry sources.

INADEQUATE INTERNAL CONTROLS

Next, I would like to comment on the problem of internal controls over data processed through computer systems. "Internal control" is the phrase we accountants use to describe the system of checks and balances that are designed to protect against theft and error. A simple example is the long-honored practice of having two people sign checks. By having 2 signatures, one person has a far greater difficulty in fraudulently obtaining funds for his personal use.

The truth today in most automated systems is that no one signs checks. The signature is simply printed on the check by the computer. Obviously, when a control like double signature is given up in favor of no signature, some new controls are needed as substitutes. There are a host of such controls but they are not always used in computer systems because they take up computer time, storage, or have other effects that cost money and sometimes produce delays in getting the work out.

As an example, let's look at the way in which Federal disbursements were processed a few years ago and how they are processed today in the most modern computer systems.

In the old manual system days, those with responsibility for preparing checks could maintain close supervision over the pay clerks, voucher examiners, and similar employees who computed and/or verified the correctness of payments or transactions. They could see to it that these employees examined the source documents supporting each payment and made sure that

--each transaction was supported by proper documentation (a purchase order, a receiving document and the vendor's invoice) and was not obviously improper or incorrect;

--each document had been properly approved and processed through all the required steps and was complete;

--the data in the various documents was consistent;

--all computations were correct; and

--the transactions complied with the laws, rules, and regulations which they were responsible for enforcing.

However, in many of today's automated systems, most of this work is done by the computer. The documents often aren't even physically at the same location. Under such circumstances, the controls to prevent fraudulent input into the system, becomes very important. For if the controls don't prevent such input, it is unlikely to be detected at all because the transactions do not receive a detailed review by a human supervisor.

In fact, literally millions of Federal actions take place regularly on automated systems without anyone checking them for correctness. For example, amounts due employees for salary payments are calculated inside the computer system, unseen by human eyes. Parts for aircraft, ships and other equipment are ordered by the computer without human verification of the amounts ordered or the price to be paid.

Despite the need for such controls to supplant those given up when the systems were computerized, Government Managers have not insisted that the appropriate controls be installed. In fact, much education is needed to get managers to take advantage of such controls. We found in many of the computer crimes we reviewed that managers placed more emphasis on making the new automated systems work as soon as possible rather than on designing control over them. For example, one crime involving a social compensation system, the computer operation was built around second-generation computers and had no fraud-oriented controls built in. When the agency converted to more modern equipment, the system was not redesigned because of pressure to get the new computers running. An employee submitted fraudulent claims to this system, and the automated system sent the checks totaling over $15,000.

Our findings with regard to the need for better controls have been reported to the Congress principally in the three reports listed below.

--Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government (FGMSD-76-5, April 23, 1976).

--New Methods Needed for Checking Payments Made by Computers (FGMSD-76-82, November 7, 1977).

--Challenges of Protecting Personal Information in an Expanding Federal Computer Network Environment (LCD-76-102, April 28, 1978).

Some action is being taken in regards to better controls over computer systems. Actions include

--the drafting and issuance of policy guidance by the central management agencies [1] on improving controls and developing a implementing computer security programs, and

--the strengthening of control over the computer systems at some Federal agencies.

Getting better controls over computer systems is important, but controls alone doubtless will not solve the fraud and abuse problem, History has shown that it is

[1] Office of Management and Budget draft TM No. 1 to OMB Circular A-71 on policy guidance for developing and implementing a computer security program.
National Bureau of Standards Federal Information Processing Standard Publication 31, titled "Guidelines for Automatic Data Processing Physical Security and Risk Management".
National Bureau of Standards special publication 500-24 on performance assurance and data integrity practices.

difficult to keep up with the inventiveness of some of the persons who seek to obtain money and other valuables fraudulently. Therefore, we believe a strong deterrent in the form of punishment--like that included in S-1766--is also needed to protect the Government's computers and others from fraud and abuse.

Mr. Chairman, this concludes my prepared statement; we will be pleased to try to answer any questions or furnish additional information.