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

FOR RELEASE ON DELIVERY
EXPECTED AT ~~10:00 A.M. EDT~~
WEDNESDAY, SEPTEMBER 28, 1977

STATEMENT OF
DONALD L. SCANTLEBURY, DIRECTOR
FINANCIAL AND GENERAL MANAGEMENT STUDIES DIVISION

BEFORE THE

SUBCOMMITTEE ON CONSUMER AFFAIRS HSE05401

COMMITTEE ON BANKING, FINANCE AND URBAN AFFAIRS

HOUSE OF REPRESENTATIVES

CONCERNING THE [SECURITY OF COMPUTER SYSTEMS]

~~709723~~
094676

MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE:

We are pleased to be with you today to discuss our views and concerns on the security aspects of computerized systems. With me today is Mr. Walter L. Anderson, Associate Director, from our Financial and General Management Studies Division.

My testimony will summarize two studies that we have reported on to Congress. One on "Computer-Related Crimes in Federal Programs" and the other on "Managers Need to Provide Better Protection For Federal Data Processing Activities."

In discussing this area the term "computer security" is frequently mentioned. I define computer security as a set of policies, procedures, and practices which are designed to assure that

--unauthorized uses of data processing resources (i.e. hardware, software, and data) are prevented or at least significantly inhibited; and

--authorized uses of these resources are carried out as reliably, accurately, and with as little interruption and loss as possible.

I would like to emphasize at the outset that we believe the computer security area is so significant that it demands

top management attention. The potential results of a poor security program can be catastrophic. I'm not trying to sound like a doomsdayer -- I'm merely trying to point out its significance. As I discuss our study results I think you will see why we are so concerned about the potential for major theft, fraud, misuse, and loss of assets through the use of computer systems.

As an aside, you will also note that our studies concerned computer systems in Federal Government and contain no reference to electronic fund transfer systems developed and operated by financial institutions. (As you know we have no audit authority over these institutions.) However, we believe our findings should also apply to EFT systems since they also rely extensively upon computers.

COMPUTER USE IN FEDERAL PROGRAMS

The Federal Government is the largest user of computers in the world. We estimate the Federal Government's annual cost in computer systems is over $10 billion.

Year after year more Federal programs and functions have been computerized. From a modest start of two computers in 1950 we have now grown to an inventory of 10,000 in June 1977. To help place the Government reliance on computers in proper perspective, it has been said that some agencies would find it

impractical, if not impossible, to accomplish their missions without computer systems. To illustrate, the Social Security Administration probably could not carry forth its programs without computers which are used to make payments of over $80 billion annually.

WHY DO COMPUTER SYSTEMS NEED PROTECTION?

Because of the nature and tremendous capabilities of computers, agencies have tended to centralize their computer operations in major computer centers. This centralization increases the potential for major thefts, frauds, misuses, or loss of personal privacy. Consider for a moment the possibility of:

--Large amounts of government funds being paid out for fraudulent claims;

--Valuable information being stolen;

--Information or records being destroyed, altered, or misused;

--Harm being done to individuals by improper use of personal information collected and maintained, and

--The potential for criminal abuse.

WHAT DID WE FIND?

In our two studies of computer crimes and physical security, we found that Government computer systems were not being properly protected because many installations lacked important security and control measures.

Some effects that have occurred because computer systems and installations are vulnerable and not properly protected include:

--Losses of equipment, software, data, and buildings;

--Losses of funds;

--Personnel injuries; and

--Loss of life.

Some of these losses were minimal, while others were catastrophic.

We have categorized our findings into the following two categories: Criminal Actions and Physical Security Problems.

Criminal actions

This includes such actions as crimes, espionage, mischief, and sabotage. Our April 27, 1976, report on computer crimes (FGMSD-76-27) addresses these acts.

We can best illustrate the varied types of crimes by giving some examples of cases gathered from agency records.

The majority of cases--about 62 percent--involved persons preparing fraudulent input to computer-based systems. Several variations of this method have been discovered.

All types of systems (personnel, supply, social security) are particularly vulnerable to fraudulent input. In one case, a perpetrator used a computer terminal to

ascertain 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. He used these documents to obtain the items he wanted, and he later sold them to outside parties. Although the total amount of property stolen through computerized supply systems cannot easily be determined, the value of one such theft in our case files was about $53,000. Another loss of over $300,000 was averted when discrepancies were discovered accidentally and the material recovered.

Many cases in which individuals prepared fraudulent input involve systems that make direct payments to individuals or businesses. These include fraudulent payroll, social welfare, and compensation transactions as well as payments for nonexistent goods and services. For example:

--A Government employee who had helped automate an accounting system introduced fraudulent payment vouchers into the system. The computer could not recognize that the transactions were fraudulent and issued checks payable to fictitious companies set up by the employee and his accomplices. These checks were sent directly to banks where the conspirators had opened accounts for the companies. The criminals then withdrew the funds

from the accounts. Officials estimated the Government may have paid this employee and his accomplices $100,000 for goods that had never been delivered.

--A supervisory clerk responsible for entering claim transactions to a computer-based social welfare system found she could introduce fictitious claims on behalf of accomplices and they would receive the benefits. She was able to process over $90,000 in claims (authorities believe it might have been up to $250,000) before she was discovered through an anonymous telephone tip.

Another type of act, which has occurred in several agencies, is the unauthorized use of computers by ADP personnel. An engineer who was no longer employed at a computer 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 monetary losses. The manager of a non-Federal computer center processing personal information 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 was violated.

Inadequate physical security protection

Computerization tends to centralize Government assets and data, making them more vulnerable to destruction or alterations than ever before. We found a number of conditions at several Government installations which led us to believe that physical security was not adequate and that action should be taken to protect against possible losses caused by fire, flood, fraud, theft, embezzlement and human errors. Our May 10, 1976, report on physical security (FGMSD-76-40) addresses this problem. I will highlight a few of the conditions along with some adverse effects of security weaknesses:

--At least five locations were susceptible to theft or misuse. We found that remotely accessed computer systems were in operation without software to detect improper or erroneous attempts to use the computers or data files involved.

--At least seven locations were susceptible to sabotage because outside service personnel were not supervised while on the premises. Three computer

locations were also possible targets for vandals. In 1970, a bomb exploded outside an Army computer facility and killed one employee, injured three others and resulted in damage to assets of $2.4 million and a loss of 20 years' accumulated data valued at $16 million.

Also, in our study of a bid protest case we found that a bidder's proposed system did not meet an agency's security specification requirements for read access protection of computer files. The bidder's proposal failed to provide adequate protection against unauthorized users accessing and reading the agency's computer programs and the computer's operating system. The protection specified in the solicitation was designed to stop users of the system from obtaining secret passwords and classified energy data they were not authorized to have. We pointed this out to the agency on July 15, 1975 (B-178205).

Nonetheless, the bidder was awarded the contract and later, in June 1976, a "computer burglar" was convicted of breaking into the classified energy files of the agency. By using a telephone, a computer terminal, and the secret passwords of authorized users of the system, the computer burglar obtained a large volume of classified energy information before being caught.

CONCLUSION

The results of our studies show an obvious need for a high level of security protection for data processing resources and the assets they control. Assets in commercial EFT systems will include the funds of consumers. These funds will no longer be solely protected by brick, mortar, and steel.

It is generally recognized in today's computer field that perfect security is not possible--all computer systems are exposed to varying degrees of vulnerability. On the other hand, many techniques have been developed to enhance the security of computer systems. One technique is data encryption. This is a method of coding data in such a complicated way that it is virtually impossible to economically interpret the data unless the special way in which it was orginally encrypted or coded is also known. In view of the potential vulnerabilities of computerized systems and the evolving fluid state of improved security practices, we believe that policy makers and management must consider the security of computer systems as a subject deserving special attention.

The protections that we recommend are outlined in our reports to Congress. In the crimes area we advocate adaptations of the good practices that have provided protection in non-automated systems. They include:

--An organizational plan that separates the duties of individuals to minimize opportunity for misuse or misappropriation.

--A system of authorization and record procedure to provide accounting control.

--An established system of practices for each duty and function of the organizational element.

--An effective system of internal review.

To attain the highest levels of physical security at practical costs we recommend a risk assessment method. This is a process by which actual and potential threats are analyzed to determine the proper types and levels of protection required to attain an acceptable level of risk. However, our major recommendation is rather simple. We recommend that each financial institution appoint a high management official to be responsible for security, including both the management of security and security planning with use of risk assessment methods.

We appreciate the opportunity to testify; we will provide any further information we have that will assist you in specifying adequate consumer protection.