95th Congress }
1st Session }

COMMITTEE PRINT

STAFF STUDY OF

COMPUTER SECURITY IN FEDERAL PROGRAMS

COMMITTEE ON GOVERNMENT OPERATIONS

UNITED STATES SENATE

FEBRUARY 1977

Printed for the Committee on Government Operations

95th Congress
1st Session } COMMITTEE PRINT

STAFF STUDY OF

COMPUTER SECURITY IN FEDERAL PROGRAMS

COMMITTEE ON GOVERNMENT OPERATIONS
UNITED STATES SENATE

FEBRUARY 1977

Printed for the use of the Committee on Government Operations

U.S. GOVERNMENT PRINTING OFFICE
80-246 WASHINGTON : 1977

For sale by the Superintendent of Documents, U.S. Government Printing Office,
Washington, D.C. 20402 - Price $2.80

COMMITTEE ON GOVERNMENT OPERATIONS

ABRAHAM RIBICOFF, Connecticut, *Chairman*

JOHN L. McCLELLAN, Arkansas
HENRY M. JACKSON, Washington
EDMUND S. MUSKIE, Maine
LEE METCALF, Montana
JAMES B. ALLEN, Alabama
LAWTON CHILES, Florida
SAM NUNN, Georgia
JOHN GLENN, Ohio
JAMES R. SASSER, Tennessee

CHARLES H. PERCY, Illinois
JACOB K. JAVITS, New York
WILLIAM V. ROTH, Jr., Delaware
LOWELL P. WEICKER, Jr., Connecticut
ORRIN G. HATCH, Utah
RICHARD G. LUGAR, Indiana

RICHARD A. WEGMAN, *Chief Counsel and Staff Director*
PAUL HOFF, *Counsel*
ELI E. NOBLEMAN, *Counsel*
DAVID R. SCHAEFER, *Counsel*
MATTHEW SCHNEIDER, *Counsel*
PHILIP R. MANUEL, *Investigator*
FRED ASSELIN, *Investigator*
ELLEN S. MILLER, *Professional Staff Member*
JOHN B. CHILDERS, *Chief Counsel to the Minority*
BRIAN CONBOY, *Special Counsel to the Minority*
MARILYN A. HARRIS, *Chief Clerk*
ELIZABETH A. PREAST, *Assistant Chief Clerk*
HAROLD C. ANDERSON, *Staff Editor*

MEMORANDUM

To: Members of the Senate Government Operations Committee.
From: Senator Abe Ribicoff, chairman.

This staff study by the Senate Government Operations Committee staff addresses several problems associated with computer programs in the executive branch.

Of significant interest are problems having to do with personnel security, the awarding of federal contracts for computer services to commercial firms and strengthening the integrity of the Internal Revenue Service computerized tax return system.

In addition, the staff sought to provide information on how federal agencies secure computer systems that are involved in the disbursement of public funds, economically valuable data and personal privacy data.

The Government Operations Committee has been assured by the Office of Management and Budget, which has fiscal and policy control over computer operations in the executive branch, that this staff study will be given careful review and a response to issues raised in the staff study will be submitted to the Committee.

It is also noteworthy that OMB Director Thomas Bertram Lance, when he came before the Committee for his confirmation hearings January 17, 1977, discussed the computer issue and the staff study.

I asked Mr. Lance this question:

> The Office of Management and Budget has fiscal and policy control for computer operations in the executive branch. On May 10, 1976, the staff of the Senate Government Operations Committee began a preliminary investigation regarding problems in federal computer operations. A Committee Print entitled "Problems Associated With Computer Technology in Federal Programs and Private Industry" was issued June 21, 1976. The investigation went forward and resulted in a staff study being written entitled "Computer Security in Federal Programs." The Government Printing Office now has the staff study and it will be made public as soon as it is printed and returned to us, which should be in a few days. It is my understanding that my staff has briefed your staff on the substance of the study and provided certain sections of it to you, including the findings and conclusions and recommendations for corrective action. On the basis of this information, what is your initial response to the staff study and do you contemplate any corrective actions as proposed by the staff?

Mr. Lance replied:

> I have received the staff study mentioned in this question and presently have it under review. The central point made by the study—that the security of federal computer operations, particularly in such areas as distribution of public funds and highly private or economically valuable data should be improved—is, in my judgement, useful and valuable.
>
> I believe that the primary responsibility of establishing such safeguards in federal computer operations rests with the relevant departments and agencies. OMB's role can be both to insure that the executive branch is aware of important issues in this field and periodically to review procedures to insure security of information. Studies like the one you have forwarded to me are certainly helpful in alerting us to the most significant problems. After the study has been reviewed, appropriate actions will be taken to implement pertinent recommendations for corrective action in accordance with OMB's role as outlined above.

I found Mr. Lance's response to my question to be most satisfactory. Moreover, the Committee has been assured that OMB will provide a more detailed response to the staff study as one of its early priorities for 1977. It will be my intention to insert OMB's more detailed response in the Congressional Record or to reprint it in the form of a Committee Print. The Committee may then wish to initiate further actions in this area.

CONTENTS

- II. Computer use in Federal programs:

- III. The GAO's findings:

- IV. Personnel and physical security in computer programs:

- V. Individual agencies comment on computer problems:

I. INTRODUCTION

In April and May of 1976, the Financial and General Management Studies Division of the U.S. General Accounting Office (GAO) issued three reports on problems associated with computer technology in Federal programs.

The first report, dated April 23, 1976, was entitled "Improvements Needed In Managing Automated Decisionmaking By Computers Throughout The Federal Government."

"Computer-Related Crimes In Federal Programs" was the title of the second GAO report. It was dated April 23, 1976.

May 10, 1976, was the date of the third report, "Managers Need To Provide Better Protection For Federal Automatic Data Processing Facilities."

Each of the reports was delivered as they were made public to Senator Abe Ribicoff of Connecticut, the chairman of the Senate Government Operations Committee. The General Accounting Office, as an investigative and auditing arm of the Congress, submits its Reports to Congress to the Senate and House Committees on Government Operations, the President pro tempore of the Senate and the Speaker of the House. The GAO Reports to Congress are then made available to other interested congressional committees, Senators, and Representatives and the press and, upon request, to other parties.

On May 10, 1976, as chairman of the Senate Government Operations Committee, Senator Ribicoff announced in Senate remarks that the committee staff would begin a preliminary investigation concerning issues raised in the three GAO reports on computer problems.

The preliminary staff investigation was to examine problems associated with computer technology in Federal programs and private industry. Senator Ribicoff directed that the inquiry focus specifically on the two major issues raised in the GAO reports, computer crime, and computer security. To conduct the preliminary staff inquiry, Senator Ribicoff assigned Fred Asselin, a committee investigator, and Philip R. Manuel, an investigator from the Senate Permanent Subcommittee on Investigations detailed to the full committee.

On June 21, 1976, the Senate Government Operations Committee issued a 447-page committee print entitled, "Problems Associated With Computer Technology In Federal Programs and Private Industry."

The committee print contained the three GAO reports on computer problems, as well as articles selected at the committee's request by the Science Policy Research Division of the Congressional Research Service of the Library of Congress. The articles were selected by the Library of Congress to provide Senators with the views of experts in the field of computer technology in connection with computer abuses and computer security.

Also included in the committee print were articles selected by the committee staff reflective of a broad range of computer-related problems.

Meanwhile, the preliminary staff investigation, begun May 10, 1976, continued. The staff assembled sufficient information on computer security and computer crime in Federal programs and private industry to lead to a preliminary finding that serious problems did exist. In light of that staff finding, Senator Ribicoff directed that this staff study be issued.

The jurisdiction of the Government Operations Committee to conduct this investigation is spelled out in rule XXV of the Standing Rules of the Senate.

Rule XXV asserts that the Senate Government Operations Committee has the responsibility to receive and examine reports of the General Accounting Office and to recommend to the Senate corrective actions which may be called for as a result of information obtained by the GAO.

In addition, rule XXV directs the Government Operations Committee to study the operation of Government activities at all levels to assure economy and efficiency.

Moreover, according to rule XXV, the mandate of the Government Operations Committee also extends to matters relating to "budget and accounting measures, other than appropriations."

In each of these jurisdictional areas—GAO reports; economy and efficiency in Government; budget and accounting "other than appropriations"—there is a clear connection to computer applications in Federal programs. To a significant extent—the true measure of which no one knows—the U.S. Government could not function, as presently organized, without computers.

In turn, the Office of Management and Budget (OMB), the General Services Administration (GSA), and the National Bureau of Standards of the Department of Commerce are the three agencies in the executive branch with responsibility for establishing Government-wide policies and procedures for computer operations. Two of these lead agencies in computer matters—OMB and GSA—report directly to the Senate Government Operations Committee in the legislative oversight process.

In addition, the full committee has, by virtue of Senate Resolution 363 (Mar. 1, 1976), authority to investigate syndicated or organized crime and fraud and other irregularities in all branches of Government.

In examining the issue of computer security in Federal programs, this staff study incorporates information obtained from several departments and agencies of the executive branch including the Office of Management and Budget, the General Services Administration, the National Bureau of Standards of the Department of Commerce, the Departments of Defense, Agriculture, Justice and Health, Education and Welfare, the Federal Bureau of Investigation, the Bureau of Prisons, the Central Intelligence Agency and the Internal Revenue Service. Also included in this staff study is information provided by the General Accounting Office and a number of persons knowledgeable about computer applications who do not work for the Government.

In summary, the staff study examines findings of the General Accounting Office regarding problems and inefficiencies in computer systems in Federal programs.

Next, the staff study traces the development of computer technology and its growth in the executive branch.

Then, the staff study describes various responsibilities carried out by the National Bureau of Standards and the General Services Administration regarding automated data processing (ADP) systems in Federal programs. Special focus is placed on security procedures and policies.

To demonstrate what the committee staff feels are inconsistencies and questionable practices in Federal ADP programs, the staff study reports on information obtained in connection with a rehabilitation and training project at the U.S. Penitentiary at Leavenworth, Kans.

At the prison, inmates are trained to be computer programers. With their programing skills, the inmates then are engaged by Federal Prison Industries, Inc., an enterprise owned by the U.S. Bureau of Prisons. Under contract to the U.S. Department of Agriculture, the inmates write programs for the Agriculture Department that have to do with financial transactions that result in the disbursement of millions of dollars in public funds through programs such as the Commodity Credit Corporation and the Agricultural Stabilization and Conservation Service.

Conversely, it is the view of the U.S. Civil Service Commission, as articulated in the staff study, that personnel working on ADP projects having to do with the disbursement of public funds should be subjected to full field background checks to demonstrate a reasonable level of personal integrity and suitability to hold sensitive positions.

The Leavenworth inmates are felons, many of whom have relatively high rates of recidivism or have committed white collar crimes such as bank embezzlement and interstate transport of stolen or bogus securities or have murdered or kidnapped people.

The Leavenworth computer is also connected to the Computer Sciences Corporation's Infonet system, the time-sharing service which does about $25 million a year in business with Federal agencies including the Internal Revenue Service.

The staff study also describes how various persons, including a prisoner at Leavenworth, have apparently figured out how IRS computers evaluate individual income tax returns and have used this information to generate illegal returns for themselves and their accomplices.

The prisoner at Leavenworth, who was not enrolled in the computer rehabilitation program, filed fake returns with IRS that led the IRS computer to send him totally undeserved refunds of nearly $20,000. The prisoner, once apprehended, claimed that he was framed by a fellow prisoner who was enrolled in the Leavenworth computer rehabilitation program.

In connection with the Leavenworth aspect of the committee's preliminary staff investigation, the staff study contains an evaluation of and information about the prisoner rehabilitation project from the U.S. Bureau of Prisons and an evaluation of the Leavenworth project by a computer scientist whose specialty is computer security.

The computer scientist is Robert P. Abbott of Berkeley, Calif., who was retained as a consultant by the Senate Government Operations Committee for this preliminary staff investigation.

Abbott's previous assignments include having headed a team of computer experts under contract to the Department of Defense to pinpoint vulnerabilities in ADP systems housing national security information.

The staff study also contains information provided by the Agriculture Department on programs operated at the Department's Kansas City Computer Center, the Federal installation whose computers are on-line with the computer at the Leavenworth prison.

Space considerations compelled the staff to limit the number of individual agencies which were asked to comment on ADP security policy and procedures.

The Federal agencies which were selected were those which were deemed to have had extensive experience with computers or whose computer policies and practices were felt to be reflective of a wide range of ADP security problems and safeguards.

Accordingly, presentations on ADP security policy and problems were requested and are represented in the staff study from the Central Intelligence Agency, the Department of Defense, the Department of Justice, the Federal Bureau of Investigation, the U.S. Civil Service Commission and the Department of Health, Education and Welfare and other departments and agencies.

In turn, the staff study contains an explanation of the potential for white collar criminals and organized crime in general to exploit computers for illicit profit.

In that connection, another section of the staff study is devoted to a legal analysis of current laws which may apply in litigation involving alleged computer abuses.

Also included in the staff study are a description by Jervis S. Finney, the U.S. Attorney for the District of Maryland, of the approach he took in the successful prosecution of a major crime by computer; and a report from the IRS on what measures revenue officials are initiating to foil computer-related tax refund schemes.

The Office of Management and Budget (OMB) has the responsibility to set policy regarding ADP operations in Federal programs throughout the executive branch.

OMB Director James T. Lynn wrote the Senate Government Operations Committee on December 29, 1976 to advise the committee of steps OMB is taking in connection with improving computer operations in the executive branch.

Director Lynn's letter is reprinted in the staff study.

The staff study ends with a series of staff findings and conclusions and recommendations for corrective actions.

II. COMPUTER USE IN FEDERAL PROGRAMS

Working with the staff of the Senate Government Operations Committee, the General Accounting Office provided information relating to the growth and use of computer technology in Federal programs. This information was provided the committee September 28, 1976, in a document prepared by Donald L. Scantlebury, Director of GAO's Financial and General Management Studies Division.

WHAT A COMPUTER IS

While most Americans are affected to one degree or another by computers, many people do not know what a computer actually is and what it does. Donald Scantlebury, of GAO, said that a computer, in its simplest terms, may be viewed as a fast calculator. The computer has the added dimension of memory, logic and an enormous storage capability. A computer's functions, he said, have been succinctly defined as input-process-output.

Scantlebury said the input is the process of amassing the raw data and preparing it for acceptance by the machine. This procedure is performed by humans. The data itself comes from many sources. Scantlebury said the preparation of the data for acceptance by the machine consists of converting the human intelligible data into machine-readable coded data.

The process is the manipulation of the data according to a set of preestablished instructions already imbedded in the computer, Scantlebury said, adding that alterations to these instructions will change the results.

The output, Scantlebury said, is the resulting product from the processing of the raw data.

Thus, the equation of input-process-output demonstrates, at its most fundamental level, how a computer is, first, given data by a human; how the computer then arranges this data according to a set of instructions called its program; and, finally, how the computer reports in readable language the results of its evaluation of the data already fed into it. It should be noted that in the input-process-output equation humans can participate in and monitor the operations of the computer at each step.

Scantlebury said that in the early use of computers, data was processed and a report was generated. Changing the computer's instructions, or program, was difficult, he said. But, Scantlebury said, technology has made significant strides forward in improving the process part of the operation.

THE POTENTIAL FOR CRIMINAL ABUSE

Scantlebury pointed out, for example, that one breakthrough was the development of English-like language to write instructions for the computer. This development simplified the process of writing computer programs and instruction and allowed for greater flexibility and ease in the use of computers. This coupled with lower costs has stimulated utilization and proliferation of computer technology. He pointed out, however, that the growth of computer technology—and its availability to more and more people—is accompanied by the risk that criminals will seek to exploit this new field. "Advances in communications and teleprocessing are putting the computer at the fingertips of all kinds of potential users—legitimate and otherwise," Scantlebury said. "Today all one needs is access to a terminal and a telephone line." There is risk that criminals will probably find ways to use this new technology for illicit purposes.

A specific area of potential exploitation by criminals, Scantlebury said, can be seen in the widespread use of computers to store huge amounts of financially viable data. These data banks are so designed as to be readily accessible to legitimate parties, Scantlebury said, acknowledging the possibility, however, that persons without a legitimate interest may also gain unauthorized access to this data.

COMPUTERS INCREASED AS GOVERNMENT GREW

The Federal Government is the largest user of computers in the world. GAO estimated that the Federal Government's annual cost in computer systems is more than $10 billion. Moreover, independent inquiry by the committee staff, corroborated by GAO, found that the Federal Government today, as presently organized, could not function without computers. As Donald Scantlebury asserted, "Computer systems have become an integral part of the Government process by performing many of the operations and applications that, in the past, were not done at all or were done manually. Some agencies would find it impractical, if not impossible, to accomplish their missions without computers."

In turn, the rapid growth of computer technology in Federal programs has coincided with the growth of Government itself. According to the GAO, in 1950, the Federal Government had two computers, 2 million civilian employees, and a $40 billion budget.

From 1950, the Nation has witnessed large increases in social programs, Government services—and computer systems.

GAO's Donald Scantlebury said the cost of this increased service and workload is demonstrated in the 1977 Federal budget of about $400 billion. In less than 30 years, he said, the Federal budget has increased tenfold. But, Scantlebury noted, there has been no corresponding increase in Government personnel. The full-time civilian work force in Government for 1977 is less than 2.5 million—a 25-percent increase over 1950, Scantlebury said, adding that this civilian work force today relies on nearly 10,000 computers to help them run the Government. This represents a 5,000-fold increase over 1950.

"This is a very simple comparison I'm making," Scantlebury said, "obviously I'm not saying that computers alone have kept the work force more constant than the budget, but they have had a significant impact."

Chronology of Computer Use in Federal Programs

According to information provided the committee by the General Accounting Office, the first computers installed in the Federal Government were used primarily to support Department of Defense research projects in the period from 1950 to 1955. In 1951, the Bureau of the Census of the Department of Commerce installed a computer to compile census data. This was considered the first business-type computer application.

From 1955 to 1960, the number of computers in use in the Federal Government increased from 45 to 531. Computers continued to be used in scientific projects but their application was expanded markedly as this rapidly growing technology began to be applied in Government programs to pay old-age and survivors benefits by the Social Security Administration; to account for pension payments by the Veterans' Administration; to gather weather forecasting data by the Commerce Department; to provide personnel management information at the Defense Department and the National Institutes of Health; to manage military material and supply inventories; and to accumulate labor statistics for the Department of Labor.

In the period from 1960 to 1965, computer use continued its rapid growth, numbering about 2,500. This increase resulted from greater applications of this technology in research and material management.

The Veterans' Administration began using computers to process insurance program data while the General Services Administration's computers prepared bills of lading and Federal Telecommunications System billings.

At the Internal Revenue Service, computers began processing tax returns and the U.S. Patent Office turned to computers to automate patent searches.

The Defense Department found many roles for computers, utilizing them in missile and air defense systems, in processing intelligence, in evaluating petroleum bids and in procurement procedures. Similarly, the National Aeronautics and Space Administration came to rely heavily on computers in controlling missions.

The number of computers in use by the Federal Government went up from 2,412 in 1965 to 5,277 in 1970. This increase, according to GAO, was attributable to the expanded use of computers in financial and administrative operations as well as stepped-up use in research and development.

In this 5-year period, the Defense Department was applying computer technology to maintain flight records and passenger reservations, to analyze satellite weather data, to standardize and integrate personnel and financial systems and to assist in assigning and training personnel. The new technology was applied in this Nation's military effort in Southeast Asia. For the first time, the computer had gone to war.

Computers at the Department of Housing and Urban Development managed housing grants. At the Treasury Department, they issued savings bonds. The post office processed money orders with computers and the Department of Agriculture used them to predict crop levels.

The Department of Justice and its Federal Bureau of Investigation stored and retrieved criminal data with computer systems. And the General Services Administration and the Department of Transportation managed inventories with them.

By 1976, computers were being used in virtually all Federal agencies. Computers were reporting on title I home improvement loans at the Department of Housing and Urban Development. They were automating air traffic control functions for the Federal Aviation Administration at major airports. The Department of Justice was using computers in the awarding of grants. The Agriculture Department was relying on computers in the Agricultural Stabilization and Conservation Service and the Commodity Credit Corporation. The Congress was keeping track of proposed legislation with computers. The U.S. Supreme Court called upon computers to assist in the processing of judicial records. In short, the computer had become an essential and growing tool throughout the U.S. Government.

Demonstrative of the Government's dependence on computers are these observations by GAO's Donald Scantlebury:

> You . . . see that year after year more programs and functions were computerized. From a modest start of two computers in 1950, we have now grown to an inventory of 9,500 in June 1976. To highlight their importance, the National Aeronautics and Space Administration could not carry out its space programs and the Federal Aviation Administration could not control aircraft effectively without computer assistance. Many computer systems are used by the Social Security Administration to create checks for social security payments of over $84 billion annually. The Internal Revenue Service also uses computer systems to process about 125 million income tax returns each year. The agencies mentioned here, NASA, FAA, Social Security, and IRS—are only examples of agencies that are very dependent on computers to carry out their programs. There are many others that could continue to function but only at reduced levels of efficiency and effectiveness if computers were not used.

CONGRESSIONAL INTEREST IN COMPUTERS

Congressional interest in computers in Federal programs remains a critical part of the legislative goal of better resource management. Since computer systems are costly and since they have become inseparable from Federal programs, there has been continuing congressional monitoring of this relatively new technology.

The General Accounting Office, for example, has, since the 1950's, issued several reports detailing the need for improved management of automatic data processing activities. These reports dealt with the acquisition, procurement, management, and use of these computer systems.

In the early 1950's, the House Appropriations Committee asked GAO to study and report back on the development and use of punch card equipment. In the late 1950's and early 1960, the House Post Office and Civil Service Committee examined the effects of computer systems on Federal employment.

In turn, the House Government Operations Committee during the past 15 years held many hearings on the acquisition and use of computer systems by Government. The enactment in 1965 of Public Law 89–306—commonly referred to as the Brooks bill after House Government Operations Committee Chairman Jack Brooks of Texas—resulted from these hearings.

The Joint Economic Committee was concerned about economy in the procurement of data processing equipment in the early 1970's, Scantlebury said, adding that many other Senate and House Appropriation Committees have held hearings dealing with the most efficient and effective way to acquire and utilize computer systems. Recently, the right to privacy has been the subject of many congressional hearings and legislation, one of the most significant results of which was the Privacy Act of 1974, Public Law 93–579. The principal sponsor of the Privacy Act was former Senator Sam Ervin of North Carolina, who was chairman of the Senate Government Operations Committee.

THE "BROOKS BILL" AND THE PRIVACY ACT

The preliminary staff investigation by the Government Operations Committee, initiated May 10, 1976, by Senator Ribicoff, examined computer technology in Federal programs and private industry but its primary focus was on computer-related crime and computer security. While there has not been any computer related crime and security legislation passed by the Congress in the past 25 years, two laws have been enacted which have an impact in this area. They are the "Brooks bill," Public Law 89–306, and the Privacy Act of 1974, Public Law 93–579.

The Brooks bill, enacted October 30, 1965, provided for "the economic and effective purchase, lease, maintenance, operation, and utilization of automatic data processing equipment by Federal departments and agencies."

The Brooks bill provides that the Office of Management and Budget (OMB) exercise fiscal control and policy guidance. The General Services Administration (GSA) is to be responsible for computer equipment procurement and maintenance functions. And the National Bureau of Standards (NBS) in the Commerce Department is to give technological advisory services and establish automatic data processing (ADP) standards.

In the 93d Congress, the Privacy Act of 1974 was passed to "safeguard individual privacy from the misuse of Federal records." The law permits individuals access to records maintained by Federal agencies concerning themselves.

Under the Privacy Act, the Office of Management and Budget was designated to "develop guidelines and regulations for the use of the agencies" and to provide continuing assistance in the implementation of the law. According to a report provided the Senate Government Operations Committee by the Science Policy Research Division of the Congressional Research Service of the Library of Congress, as an initial step in implementing the Privacy Act, OMB drafted guidelines to provide agencies with an overall framework within which to identify specific administrative procedures in keeping with the law. In addition, GSA and NBS were directed by OMB to provide the executive branch specific guidelines, the Library of Congress report said. Louise Giovane Becker, analyst in information sciences, prepared the Library of Congress report for the committee. Entitled "Computer and Information Security in the Federal Government: An Overview," the document is dated June 11, 1976, and is reprinted in the Government Operations committee print of June 21, 1976.

Specific provisions of the Privacy Act which relate to computer security include (1) limiting disclosure of personal information to authorized persons and agencies; (2) requiring accuracy, relevance, timeliness, and completeness of records; and (3) stipulating the use of safeguards to insure the confidentiality and security of records.

The General Services Administration, in its response to the Privacy Act, was to develop records management procedures to help agencies implement the act. As called for in the Act, computer security requirements were to be evaluated prior to the procurement of new computer equipment or systems.

The critical responsibility for establishing norms for computer security fell to the National Bureau of Standards. These norms were set forth in June of 1974 in an NBS document entitled "Guidelines for Automatic Data Processing and Risk Management." This document is also identified as "Federal Information Processing Standards Publication 31" or, by its acronym, "FIPS 31."

At this writing, FIPS 31 is the most comprehensive document the Federal Government has issued on the subject of Government-wide efforts to curtail computer-related crimes and abuses and to protect computer installations against physical damage and unauthorized penetration and access to data.

However, independent inquiry by the Government Operations Committee staff found that procedures to prevent crime and insure security as called for in FIPS 31 are not binding on any Federal agency. At best, the procedures contained in FIPS 31 are guidelines—recommendations for action—but there is nothing mandatory about them. Nor is any agency required to assign a given office or official within that agency the responsibility for seeing to it that the FIPS 31 procedures are followed. The National Bureau of Standards, in fact, when it promulgated FIPS 31, made clear that the document constituted a series of recommendations, and little else. NBS asserted in the FIPS 31 summary, "The essential recommendations from this publication are summarized here to show the scope of these guidelines and to provide a quick overview of action items in establishing, implementing and maintaining a physical security program in an ADP facility." Independent inquiry by the committee staff found that the National Bureau of Standards was neither authorized nor inclined to enforce FIPS 31. In short, no mechanism existed in the executive branch to require compliance.

Accordingly, independent investigation by the committee staff, revealed that FIPS 31 procedures were not resulting in adequate safeguards against computer crime; nor did FIPS 31 recommendations insure that reasonable safeguards against physical damage and unauthorized access to data were being implemented. In certain instances, in fact, the committee staff found that FIPS 31 recommendations were not being applied. In addition, the committee staff noted, since the FIPS 31 procedures were recommendations only and were not backed up by any Government-wide compliance mechanism, individual agencies were being left to their own devices on the issue of computer security. Security measures were varied and diverse and without consistency, ranging from very severe precautions such as those employed at the Central Intelligence Agency to questionable procedures followed by the U.S. Department of Agriculture which contracted for the services of imprisoned felons to program computer general ledger and other financial data for USDA's Commodity Credit Corporation and Agricultural Stabilization and Conservation Service. Similarly, the Department of Health, Education and Welfare's Office of Investigation had no personnel with training in computer fraud detection and investigation.

However, HEW, which has the largest budget of any Federal agency—and which relies on computers in the expenditure of some $84 billion in health, education, and welfare payments—assured the committee that it is taking steps to strengthen its investigative capability in the computer field. The issue of training Federal agents to investigate instances of computer fraud, not only at HEW but in other agencies as well, is examined in other sections of this staff study.

III. THE GAO's FINDINGS

WHY COMPUTER SYSTEMS NEED PROTECTION

In his September 28, 1976, report to the Senate Government Operations Committee, Donald L. Scantlebury, Director of the Financial and Management Studies Division of the General Accounting Office, discussed the need for providing adequate security for computers used in Federal programs.

Scantlebury pointed out that of more importance than the concern over the cost of a computer facility is the value of the information contained within the computers themselves. He said that computer technology lends itself to centralization; that is, individual computers are capable of storing large amounts of data in one place. The more sophisticated the computer, the more data it can store, manipulate and report upon. For that reason, Scantlebury said, Federal agencies have tended to centralize their computer operations in a relative few major computer centers. Scantlebury said this centralization increases the potential for major thefts, frauds, abuses and damage due to fire, flood, earthquake, vandalism, or terrorism.

Among the losses which a major Federal computer center can sustain, Scantlebury said, are (1) large amounts of Government funds being paid out for fraudulent claims; (2) valuable information being stolen for monetary gain; (3) information or records being destroyed, altered or misused; and (4) harm being done to individuals by improper use of personal information collected and maintained.

Scantlebury said each Federal computer is unique. In turn, he said, threats to its security are varied, relating directly to its purpose, use, location, work force, physical facilities and other variables. In addition, Scantlebury said, the relative risks of a facility can change over time because of changes in Government policies, laws, conditions or changes in the environment or physical situations. "Such changes," he said, "might be due . . . to war, changes in the attitude of the American people or economic conditions of the country. In any event, changes in Government policy or even the environment of the land can change the posture of a Government computer installation or decrease the the threat against it."

RISK MANAGEMENT

It was the finding of the committee staff that most computer experts are of the opinion that no installation or computer system can ever be made completely safe against crime, physical damage or unauthorized access to data. Scantlebury himself noted that, "Providing total protection against all possible threats could require unlimited funds or resources."

He noted, however, that computer systems and installations can be made reasonably secure, at reasonable cost, if appropriate management techniques are used. The approach Scantlebury proposed—and one put forward by many other computer experts—involves the concept of "risk management."

According to the concept of "risk management," Scantlebury said, a reasonable level of computer security can be achieved when Federal officials assess their computer security requirements by (1) analyzing the risks involved; (2) summarizing risk findings for management use; (3) involving high level management in the decisionmaking process; (4) implementing the most cost effective security practices to control unacceptable risks; (5) periodically reevaluating the potential impact of threats to assess values and mission accomplishments; and (6) deciding on new or existing practices to handle the risks.

After evaluating Federal computer operations, Scantlebury said, the GAO had concluded that security was not sufficient in many programs. Federal agencies were not using the "risk management" concept or other security concepts effectively.

Drawing upon information obtained for the three GAO reports on computer security issued in the spring of 1976, Scantlebury said:

> . . . Government computer systems and their applications were not being properly protected because many installations lacked important security and control measures and/or recovery procedures for continuity of operation.

The three GAO reports cited by Scantlebury were reprinted in the Senate Government Operations Committee Print of June 21, 1976. In Senate remarks May 10, 1976, Senator Ribicoff, chairman of the committee, summarized the findings of the reports. Senator Ribicoff's summary was reprinted in the committee print. In his September 28, 1976 report to the committee, Scantlebury also commented on the reports and their findings.

AUTOMATED DECISIONMAKING BY COMPUTERS

The first of the three GAO reports, dated April 23, 1976, is entitled, "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government."

"Automated decisionmaking by computers" occurs when computers are programed to make payments, purchase materials and otherwise spend money and take actions without the assistance or review by people.

Of automated decisionmaking by computers—and of its potential for initiating waste of Government resources—GAO's Donald Scantlebury had this to say:

> The power of the computer is particularly well suited to applications in which repetitive transactions based on preestablished criteria are needed. Literally millions of Federal actions take place daily based on such computer-generated operations without anyone checking them for correctness.
>
> For example, if issuance of material from inventory causes the balance of stock on hand to drop below the reordering point, a purchase order can be generated automatically by the computer. Again, based on information supplied to the computer, it can decide whether usable material turned in

> to supply by an organization should be scrapped or returned to inventory. Many such actions are taken without any manual [human] review of the computer's calculations, and great volumes of workload can be processed in this manner, contributing to greater governmental effectiveness and efficiency.
>
> However, if the computer program processing the work has errors in it; or if there is incomplete or incorrect information input to the computer; or if data already in the computer is not accurate, complete and current, the transactions will still be turned out in great volume, but they may be wrong, and they probably will not be caught.
>
> Wrong transactions can cost money and our [April 23, 1976] report points out that hundreds of millions of dollars have been unnecessarily spent as a result of such operations.
>
> Therefore, the most important point in our report is that poorly controlled systems have the potential for issuing unreviewed payments and other actions involving billions of dollars in Government assets.

In their April 23, 1976, study of automated decisionmaking by computers, GAO auditors concluded that these kinds of computer operations initiate more than 1.7 billion payments and other actions by Government a year without any person evaluating whether they are correct or not.

Government automated decisionmaking computers issue each year a minimum of unreviewed authorizations for payment or checks totaling $26 billion, excluding payroll checks, the GAO report said.

Unreviewed bills totaling at least $10 billion are issued annually by automated decisionmaking computers, the GAO auditors said. These same computers issue annually unreviewed requisitions, shipping orders, repair schedules and property disposal orders for material valued at $8 billion.

GAO obtained information on 128 automated decisionmaking computer programs at the Army, Navy, Air Force, Defense Supply Agency, General Services Administration and the Departments of Agriculture, Commerce, Housing and Urban Development, Interior, Treasury, and Health, Education, and Welfare.

The GAO auditors cited examples in which automated decisionmaking computers had resulted in millions of dollars of waste and, in one instance, the unauthorized handling of radioactive components for military equipment.

In 1969, the GAO report said, the Navy's own auditors found that a computer program serving the Navy Aviation Supply Office in Philadelphia was inadequately designed regarding the ability to correctly reflect demand for the purchase and repair of naval aircraft and spare parts. The Aviation Supply Office in Philadelphia was the central manager for all the purchases and repair of naval aircraft and spare parts.

The inadequacy in the automated decisionmaking computer program at the Aviation Supply Office was not corrected. The problem was noted for the second time on May 21, 1974, in a GAO report entitled, "Better Methods Needed for Canceling Orders for Material No Longer Required."

Again, however, the inadequacy was not corrected and the decisionmaking computer continued to inaccurately reflect demand for new equipment and for repairs on naval aircraft. Finally, 5 years after the problem was first detected, the needed correction was made. "At least $3 million in annual unnecessary costs were initiated by automated decisionmaking applications using this overstated demand data," GAO auditors said.

Design of the automated decisionmaking computers at the Aviation Supply Office was developed at the Fleet Material Support Command, Mechanicsburg, Pa., which also reported to the Naval Supply Systems Command in Washington.

GAO asked Navy officials why it had taken so long to correct the computer inadequacy. The GAO report said:

> The reasons cited by Navy officials for the 5-year delay in initiating the modifications included:
>
> Disagreements within the Navy on whether all canceled requisitions should result in reducing work demand.
>
> High priority workload at the design activity mandated by higher headquarters levels in both the Navy and Department of Defense; and
>
> Lack of pressure placed on the Navy command and design activity by the inventory control points since *reduced demands could result in budget reductions*. [Emphasis supplied.]

The Veterans' Administration (VA) used automated decisionmaking computers to make monthly payments to more than 185,000 veterans in apprenticeship and other on-the-job training programs, GAO said in its report. The VA computers were supposed to be programed to make payments at a rate that decreases every 6 months, under the assumption that an individual veteran's pay from his employer will increase as he learns his trade.

Annually, the VA computers processed about 1.4 million unreviewed checks for more than $225 million in apprenticeship and other on-the-job training benefits. However, the data submitted to the computers was incomplete and, GAO auditors said, checks went out at the highest levels to the veterans and no progressively declining payment system was implemented. The result, GAO said, was potential overpayments of $700,000.

Code 8 is the designation the Army gives its equipment and spare parts which have radioactive components and which, therefore, are required to be handled by authorized personnel in a stipulated manner.

GAO said it obtained from the Army Audit Agency data concerning the Army Electronics Command, Fort Monmouth, N.J., which processed each year at least 250,000 requisitions for material valued at a minimum of $250 million. About 35 percent of the requisitions were reviewed by people, GAO said, and the remaining 65 percent were processed by automated decisionmaking computers without review by people.

The Army Audit Agency examined 86 radioactive commodities handled by this command's automated decisionmaking computers and found that 18 of the commodities were processed not with the radioactive designation of code 8—but instead carried a code 0 rating. Code 0 means that no special controls or handling are required, GAO said.

GAO auditors said another 11 radioactive commodities were categorized as code 1, the code that indicates that the item is scarce, costly or highly technical—but not that it is radioactive.

The Army Audit Agency also studied the application of automated decisionmaking computer technology at five Army inventory control points. The Army auditors found the computers were often in error in deciding where material should be shipped. The result, the Army auditors showed, was an annual loss of $900,000 in unnecessary computer costs. In addition, a total of $1.3 million was incurred by the Army in the early 1970's due to unnecessary inventory increases caused by errors in these same computers.

The GAO report said that a major cause of inaccurate computer tabulations in the Government is the massive amounts of information fed into the machines which lead input preparers—that is, computer personnel—to make mistakes.

GAO noted, for example, that the Navy Aviation Supply Office in Philadelphia received about 10 million transaction reports each year, all of which are then fed into computers. Transaction reports are mainly prepared by Navy facilities that receive, store, and issue aeronautical equipment.

GAO auditors also estimated that during a 12-month period the VA hospital in Philadelphia prepared more than 4 million documents for insertion into computers.

To insure more accurate computer calculations, GAO proposed that the Government require selective or cyclical monitoring of actions directed by automated decisionmaking computers. The GAO also recommended that outside auditors or independent design teams from elsewhere in a given agency be called in to study the design of a computer program before it is allowed to begin making automated decisions.

Summing up the GAO report, Donald Scantlebury said shortcomings in Federal automated decisionmaking by computers could be attributed to two basic types of errors—data errors and program errors. He recommended corrective actions that included (1) management assurance that computer systems have been properly designed and tested before—not after—they were placed in operation; and (2) periodic testing of output for accuracy after the systems have been made operational.

The GAO report on automated decisionmaking by computers in Federal programs was issued April 23, 1976. On May 29, 1976, James T. Lynn, Director of the Office of Management and Budget, sent a memorandum to the heads of the Government's departments and agencies.

In his memorandum, Lynn said that the GAO report should be read by top management. Lynn then requested that each agency:

> (1) Review each of your computer operations to determine whether any of them involve automated decisionmaking applications as defined in the GAO report.
>
> (2) Review all administrative procedures, criteria, computer programs, et cetera, pertaining to such automated decisionmaking

applications to assess the possibility and probability of improper actions, the extent to which improper actions have or may be occurring and the monetary value of these improper actions.

(3) Identify and implement any improvements necessary to minimize the future occurrence of improper actions and correct improper past or pending actions where possible and appropriate.

(4) Review and analyze your existing policies, responsibilities, and procedures relative to the design, development, test, evaluation, and approval of automated processes to assure maximum efficient, effective, and economical utilization of such resources and develop any new policies, procedures, guidelines, or methodologies as necessary.

(5) Provide the results of your review and a description of corrective steps taken, underway, or planned as part of the narrative to the fiscal year 1978 ADP budget, to be submitted in fall 1976.

"With your assistance and continuing attention to this issue", Lynn concluded, ". . . we can work toward effective use of technology to maximize efficiency and effectiveness of Government operations."

Computer-Related Crimes

Its second report on problems associated with computer technology in Federal programs was issued on April 27, 1976, and was entitled "Computer-Related Crimes In Federal Programs."

The General Accounting Office was faced with a procedural problem in preparing this report, Scantlebury said, because Federal agency records do not classify computer crimes as a separate category. But, he said, "with some digging," GAO auditors were able to isolate, identify, and describe 69 individual cases in which computer-related crimes had occurred in Federal programs. The committee staff evaluation of the 69 crimes and the staff's own independent inquiry led committee investigators to conclude that this GAO report was useful only in identifying the opportunities for computer-related crime but in no way was reflective of the number of such crimes which have occurred in the past and are occurring now. Similarly, Scantlebury himself said, "No one knows how many millions of dollars have actually been lost as a result of fraudulent claims to Government systems."

Computer-related crimes in Federal programs, Scantlebury said, could be categorized in four areas: (1) introduction of fraudulent records into the computer system; (2) unauthorized use of facilities; (3) alteration or destruction of information files; and (4) stealing checks, data, or information. The 69 cases of computer crime, then, should be viewed as demonstrative of one or more of these four categories and were not meant to reflect the scope of the problem. In addition, the committee staff learned of another constraint limiting this GAO report. This constraint can be seen in the fact that all 69 cases had either been adjudicated in court or definitively resolved in an administrative or some other procedure. The result was that the cases examined by GAO tended to be old—some of them going back 4 or 5 years—and, consequently, of less public impact upon disclosure in the GAO format of presentation. Finally, the committee staff found, GAO auditors, in order to have access to original and raw documents—particularly in those cases which did not result in prosecution but were resolved in some other manner—had to make agreements with executive branch criminal investigators and other officials. The agreements were to the effect that the information the GAO would make public about the 69 cases would be general, sometimes vague, and almost never specific as to names of violators, administrative actions taken, and other pertinent data.

The General Accounting Office, examining computer-related crime in Federal programs, studied 69 individual cases that together totaled more than $2 million in losses to the Government.

The GAO inquiry revealed that computer fraud is a growing problem in both the Government and private sector and that, in many instances—no one knows how many—it is almost impossible to detect.

GAO obtained its information from the investigative files of the Criminal Investigations Division (CID) Command of the Army; the Navy Investigative Service (NIS); the Office of Special Investigations (OSI) of the Air Force; the Justice Department's Executive Office of U.S. Attorneys and the FBI; the Office of Investigations of the Agriculture Department; the Internal Revenue Service (IRS) in Treasury; HEW's Social Security Administration; the Division of Investigations of the Interior Department; and the Investigation and Security Services of the Veterans' Administration.

In the preponderance of cases, criminal prosecutions resulted.

GAO auditors cited these instances of computer crimes in Government:

A Defense Department fuel supply 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 paid this employee and his accomplices $100,000 for goods that were never delivered.

A supervisory clerk responsible for entering claim transactions to a computer-based social welfare system found she could introduce fictitious food stamp claims on behalf of accomplices and they would receive the benefits. She processed more than $90,000 in claims before she was discovered through an anonymous tip.

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 more than $5,000 worth of computer time. At another installation, a programer used a self-initiated training program to obtain the 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, GAO auditors said.

The manager of a computer center processing personal information stole some of this data and sold it to private firms. The private firms, none of which were authorized to have such data, used the information to promote their products. GAO said that although the Government did not lose money in this case the privacy of individuals whose data records were involved was violated.

At one large Army installation officers estimated that 80 percent of all thefts may have been computer related.

GAO said most of the 69 cases studied did not involve sophisticated attempts to use computer technology for fraudulent purposes. Instead, GAO said, these were uncomplicated acts which were made easier because management controls over the systems involved were inadequate.

Forty-three of the 69 cases of computer-related crimes were classified by GAO as being "fraudulent record initiation." Under this category, GAO included cases in which Federal employees, or persons employed by Government contractors, deliberately falsified information from records and documents to be fed into computers. Also included in this category was the act of falsifying claims by reuse of supporting documents previously processed.

The second category of computer-related crimes is termed "unauthorized or inappropriate use of facilities and supplies." This category includes developing salable programs on Government computers, doing commercial work for outsiders on Government computers and duplicating files and selling them.

"Processing alteration or destruction" is the third category of computer-related crimes studied by GAO. This offense includes such crimes as sabotage or altering information in the files affecting pay, promotion or assignment, and bypassing existing controls to enter unauthorized changes.

The final category examined by GAO is "misappropriation of output." Included under this section is the misappropriation of returned checks.

Commenting on these GAO findings, GAO's Donald Scantlebury, in his September 28, 1976 report to the Senate Government Operations Committee, said the most frequent type of crime in Federal computer programs had to do with introducing fraudulent records into computerized systems. Scantlebury said there had been many instances in which persons had prepared bogus data for Government computer systems, resulting in direct payments to individuals who were not entitled to them. "These cases include fraudulent payroll, social welfare, tax refunds and compensation transactions as well as payments for nonexistent goods and services," Scantlebury said.

On the subject of computer-related crimes in Federal programs, Scantlebury concluded his remarks this way:

> In the cases we reviewed, controls—both automated and manual—should have been in place and working to minimize the possibility of criminal activity but either they were not there to begin with or, if they had been provided, they were not functioning properly. In our opinion, management has a specific responsibility to see that the assets and funds for which they are accountable are protected through a proper system of controls, and in these cases failed to provide them. This concept is not new; it is a basic tenet of management and is set forth in numerous authoritative documents.
>
> Management can meet these responsibilities by having (1) an organizational plan that segregates the duties of individuals to minimize their opportunity to misuse or misappropriate the entity's resources; (2) a system of authoriza-

> tion and record procedures adequate to provide effective accounting control over assets, liabilities, revenues and expenses; (3) an established system of practices to be followed for each duty and function the organization performs; and (4) an effective system of internal audit. This includes an internal audit staff that has training adequate to review and evaluate computer-based system controls and make such reviews when the systems are being designed and after they have become operational.
>
> We believe the guidance on internal controls, internal audit and accounting methods provided in GAO's Policy and Procedures Manual for the Guidance of Federal Agencies, and in our audit standards, gives appropriate general critieria in this area; and our report's recommendations were basically a restatement of this guidance coupled with an urging that agencies review their situations and take appropriate steps to correct identified weaknesses.
>
> If crimes do occur, they should be analyzed to pinpoint the weaknesses in management's control processes that made them possible. We believe that analyses of such crimes should be made and the results provided to managers, designers, investigators and auditors to help them strengthen their operations and procedures.

Scantlebury added that the agencies which commented on the GAO computer crime report were in "general agreement" with GAO's views and said that they would implement "appropriate corrective measures."

COMPUTER SECURITY

"Managers Need To Provide Better Protection for Federal Automatic Data Processing Facilities" is the name of the third report on problems associated with computer technology in Federal programs issued by GAO in the spring of 1976. Dated May 10, 1976, this GAO report focused on the physical security of Federal computer facilities. GAO's major conclusion was that Federal ADP facilities are insufficiently protected against fire, flood, earthquake, vandalism, terrorism, program alteration, and unauthorized access.

Commenting on May 10, 1976 in the Senate on the GAO report, Senator Ribicoff said:

> We can see the potential harm in Government's failure to adequately protect computer facilities when we consider what enormous personal tragedies would result from serious damage to the social security computerized system. Social security could not function without its computers. It is impossible to estimate the effects on millions of our elderly citizens whose livelihood depends on social security should the computers be destroyed.
>
> But the potential threat is not limited to social security. In terms of Federal revenues, for instance, imagine the havoc that would result from the destruction of Federal tax records.
>
> In addition, the number of veterans in this country is larger than ever before. Each of these men and women who served in the Armed Forces may be receiving, or may be

> entitled to receive, benefits from their military service. Valuable data and records pertaining to their military service—and the benefits that accrue from that service—are on computer tapes and, in the event of catastrophe, could be lost forever.

The GAO report said there were 9,000 computers involved in Federal programs. (At this writing, there are, according to GAO, 9,500 computers in Federal programs and in 1977 there will be about 10,000.) These computers, GAO said, are worth "many billions" of dollars. GAO said the value of some of the data which is stored and processed on these computers such as social security records is immeasurable. "Consequently," GAO said, "protecting equipment and data from unauthorized or inadvertent acts of destruction, alteration or misuse is a matter of inestimable importance."

The GAO report noted, for example, that computers are used to manage the more than 500 million transactions processed by the Social Security Administration and the 4 billion facts relating to the national population compiled and managed by the Bureau of the Census.

Catastrophic losses to Government-sponsored data processing installations such as the loss of human life, irreplaceable data and equipment have occurred, GAO said. In many of these losses, GAO said, additional security measures were implemented after the event.

GAO said information on the physical security measures employed at 28 Federal data processing facilities led its auditors to conclude that Federal data processing assets and valuable data are not properly protected.

Reflective of the amount of money Federal agencies spend on computers, GAO said, is the fact that more than $10 billion is expended each year to buy and operate Federal data processing systems.

Prior to concluding that security safeguards are inadequate regarding computers, GAO studied security procedures at 28 data processing installations of the Departments of the Army, Navy, Air Force, Agriculture, Transportation, State and Health, Education, and Welfare and the Veterans Administration. Besides the 28 Federal data processing sites, GAO auditors also studied security procedures at 23 additional Government computer installations. In addition, GAO examined automatic data processing security systems used at Government contractor sites, universities, private companies, a bank and a local government.

Eighteen of the 28 data processing installations were in the continental United States. The remaining 10 were abroad.

Among its findings that computer installations were not properly protected, GAO noted that 14 installations had combustible paper supplies or magnetic tape files which were stored in computer rooms which exposed systems to losses from fire; 3 installations had computers which were in use in areas where only portable fire extinguishers were available; one installation's computers were in operation where no portable fire extinguishers were available; 12 installations had computers which were in use above raised flooring without periodic cleaning below such flooring, constituting a fire hazard; 6 installations had computers which were in operation where master electrical power shutdown controls were not easily accessible at exit points;

10 installations had computers in operation where overhead water or steam pipes—excluding sprinkler systems—existed with inadequate provision for drainage; 2 installations had computers which were used in basements below ground level, exposing systems to potential flooding conditions; 7 installations allowed vendor service personnel near computer banks without supervision; 5 installations allowed in-house service personnel to move about without supervision in computer areas; 3 installations located computers in quarters that were vulnerable to vandals; 5 installations managed their computers in ways susceptible to theft or misuse and remotely located computer systems were in operation without controls to detect improper or erroneous attempts to use computers or data files; and 14 installations lacked contingency planning to insure continuity of operations if an event occurred that threatened security.

GAO studied instances in which major data processing facilities had been hit by terrorism, vandalism, fire or natural disaster.

GAO said attempts at sabotage of computer activities had been made by employees within data processing centers. GAO said four attempts had been made to sabotage computer operations at Wright-Patterson Air Force Base near Dayton, Ohio, during a 6-month period ending November 15, 1974, by using magnets, loosening wires on the computer mainframe and gouging equipment with a sharp tool.

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. The explosion damaged 25 buildings at the university and resulted in a total loss of $2.4 million in 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 more than 1.3 million staff-hours of effort. GAO calculated this effort to represent an investment of $16 million.

In May of 1972, a bomb exploded on the fourth floor of the Pentagon above the computer facility and caused extensive damage. The computer facility was flooded from broken water pipes and parts of it were inoperable for about 29 hours.

The computer center at the National Institutes of Health, Bethesda, Md., has experienced many computer system failures due to electrical power failures. GAO said officials of the computer center estimated that they lost a minimum of $500,000 annually from electrical power fluctuations. During a 15-week period, the NIH computer center experienced 6 major electrical power fluctuations which caused 15 computer system failures. These failures resulted in destruction of data for 375 batch processing jobs and for 2,250 remote terminal users. GAO said these power fluctuations caused replacement of electronics costing more than $94,000 in various components of the computer systems.

On June 24, 1972, water from the Susquehanna River flooded all of downtown Wilkes-Barre, Pa., and filled the basement of the post office building. Water continued rising until about 6 inches of it was on the computer room floor. About $7.5 million worth of Government computer equipment was located on raised flooring on the first floor.

Had the water risen about an inch more it would have ruined virtually all of the computer equipment, GAO said.

GAO described a 1959 fire at the Pentagon which destroyed three complete computer systems valued at $6.5 million. The fire started in a vault containing stored paper and magnetic tape and spread throughout the computer center. When the fire occurred employees were unable to reach the switch to turn off electrical power for the computer system. This created a hazardous situation for firefighting efforts.

GAO cited another example of catastrophic loss caused by fire to a Government facility, although computer records were not directly involved. In July 1973, fire broke out in the Military Personnel Records Center in St. Louis, Mo. Sections of the building housing these records were not equipped with sprinkler systems, smoke detectors or fire walls. Although the fire did major damage to papers and not computerized records, GAO said, it nevertheless illustrated how devastating the loss of irreplaceable documents and records can be. GAO said that since such records are being put on computers more and more, the problem increasingly becomes a computer security problem.

GAO said the St. Louis Records Center has been the repository for about 52 million records on military personnel actions since 1912. The sixth floor, where the fire started, contained about 22 million military personnel files or jackets. About 16.8 million of these records were lost.

Of the St. Louis fire, GAO auditors said:

> This installation's mission is to maintain these official government records and to respond to inquiries made by the Congress, other Government agencies and the taxpayer. This will now be hampered for some time because the lost records—some of which may be irreplaceable—must be reconstructed to satisfy inquiries, which is a costly and time-consuming process.
>
> While it is unreasonable to expect that there would be backup for every original record in the manual files, it is reasonable to assume that some sort of contingency planning should have been done to insure continuity of operations when a loss has occurred. Agency officials told us that a contingency plan was formulated after the fire happened.

GAO cited an instance at Kelly Air Force Base in San Antonio, Tex., in which someone altered a computer program that resulted in a $100,000 theft of Government money. Due to the computer alteration, the Air Force paid $100,000 to bogus companies for aircraft fuel never delivered. The bogus companies were established by a Government employee working at the base. The employee had in-depth knowledge of the computerized fuel accounting system which he helped develop and install. An investigation was begun when a bank contacted Air Force officials regarding suspicious banking transactions involving Government checks. GAO said the employee was arrested, convicted, and sentenced to 10 years in prison.

COMPUTER CRIME IN PRIVATE INDUSTRY

In connection with its examination of computer-related crimes in Federal programs, the General Accounting Office commissioned a study of computer crimes in both Federal programs and private industry. It was hoped that such a study would enable GAO to compare crimes against Federal programs with those which occur in the private sector.

The study was conducted by the Stanford Research Institute (SRI), Menlo Park, Calif. The person in charge of the study was Donn B. Parker, a senior information processing analyst at SRI. Parker has 26 years experience in computer programing, management of computer programing systems and application development, management of computer centers, university teaching and writing, and research in the computer field. Parker was associated with Control Data Corp., working in the aerospace industry, until he joined SRI 7 years ago. In 1966, he wrote the first code of ethics for the Association of Computing Machinery, the largest professional society in the computer field. Parker is also the author of articles and books on computers and is quite well-known in the computer science community. His most recent publication is "Crime By Computer" (Charles Scribner's Sons, 1976).

In its report on computer crime in Federal programs, GAO relied on data from the Stanford Research Institute study, but it did not recount the SRI's findings in detail. The committee obtained a copy of the SRI study.

The SRI study headed by Parker defined computer compromises in these words:

> Computer abuse, in its broadest terms, means any intentional act involving computers in which a victim suffers or could have suffered, a loss, and a perpetrator makes, or could have made, gain. This definition includes a broad spectrum of acts ranging from those that could result in criminal convictions to those where the perpetrator could have been reprimanded or fired from his job. This spectrum also encompasses cases that are disputed among businessmen where civil cases may or may not be litigated.

The SRI study examined 350 cases of computer abuse which had been reported since 1958. The sources of these reports were primarily the public media—newspapers, magazines, and trade journals. The SRI report said that about one-half of these cases had been verified by personal contact with people directly involved in the incidents. The remaining unverified cases were based on extensive documentation in some cases; other cases were based entirely on newspaper articles alone. About 20 of the cases were investigated in detail in the field at the sites where they occurred. Eighteen of the perpetrators of computer abuses were interviewed, the SRI report said.

Of the 350 cases studied, SRI noted, 50 occurred in Government—domestic and foreign. Eight occurred in the U.S. Government. SRI offered these explanations as to why so few Federal Government cases could be identified.

> . . . it is possible that fewer Federal cases are publicly reported than are cases from the private sector and from

> other levels of government. There are also indications that many incidents of losses within the Federal Government might not have been criminally prosecuted, but have been handled "administratively." This apparently is a euphemism for indicating that the perpetrators were fired, transferred, or privately reprimanded by their managers.

SRI did suggest, however, that computer abuses in Federal programs do not show up in statistics because they are, in fact, small in number in comparison to other areas of computer operations. In support of this possibility, the SRI report said, there tends to be a "paternalistic" environment in Federal employment, owing in part to U.S. Civil Service and other protections, which provide less motivation to workers to commit crimes against their employer than personnel elsewhere, particularly white collar crimes.

In turn, the SRI report said, its investigators had conducted computer security surveys at Federal computer installations and compared the results of these surveys with similar exercises in the private sector. SRI found security "is at least as poor" in Federal programs as it is in the private sector. Accordingly, SRI said the opportunity for computer crime in Federal programs and private industry was about the same. "An argument for why there should be more computer abuse in the Federal Government than in other sectors is that employees might more easily rationalize financial fraud or theft from the Federal Government because of its size and financial resources, compared to the private sector where financial resources are more closely identified with personal income," the SRI report said, thus acknowledging that its investigators had no firm convictions as to why computer compromise seemed to be more readily identifiable in the private sector than in the Federal Government.

But SRI did point out that the issue of which sector—public or private—suffered the most identifiable computer compromises was not as significant as the more important conclusion that computer systems, no matter who owns and operates them, are equally vulnerable to criminal penetration. The SRI report said:

> . . . from a computer technology point of view, there is little or no difference between computer centers in the Federal Government and computer centers in other segments of society. The hardware and software are the same. The types of environments housing computers are the same. The staffs are similarly organized. And the applications of the computers are similar in comparing similar types of business and Government functions. Therefore, on a technical basis, the carryover of what is found in the private sector should be relevant to the Federal sector.

How a computer crime is detected was a subject SRI tried to evaluate. Only 6 of its 350 cases were discovered by auditors. However, SRI's report said, crimes discovered by auditors "tend to be kept confidential" and, therefore, investigators would be less likely to learn about them. Most of the 350 cases examined by SRI were discovered accidentally because, SRI said, "the perpetrator made a mistake or curcumstances revealing the crime were beyond his control." SRI concluded that, if its data—as well as its interpretation of its data—are correct, "It can be assumed that only a small number of computer abuse cases that have occurred are being discovered and even fewer publically reported. This is based on the fact that most known cases have been discovered only accidentally and many more are treated confidentially," according to certified public accountants interviewed by SRI.

Another point made by SRI was that, in a high incidence of cases, it takes two or more violators to carry out a computer crime.

The high incidence of collusion—as compared to general white-collar crime—leads to the conjecture that when a crime is committed in a technical ADP environment that more skills, knowledge, and access are required than are possessed by any one perpetrator, the SRI report said.

As for the average loss sustained in a computer crime, the SRI found that losses per incident were far higher with computer-related white-collar crime than with other forms of white-collar criminality. For example, the study cited a 1971 survey of bank fraud and embezzlement cases. This survey, SRI said, showed noncomputer bank fraud and embezzlement to average $100,000 a case while computer-related bank fraud and embezzlement to average about $500,000 a case. In this regard, SRI said:

> The trend to larger losses when crimes involve computers might be explained by noticing that assets are generally more concentrated and easier to manipulate in large amounts in computer systems than in equivalent manual systems. Also, since the processes that are being attacked are automated, it is reasonable to believe that the crimes are also automated leading to the potential for much larger losses. Once a method for financial theft or fraud has been developed, then it can more easily be repeated in a computer environment than in a manual environment.

The Stanford Research Institute computer team, headed up by Donn B. Parker, sought to draw a profile of the kind of person who engages in a computer crime. Eighteen violators were interviewed, and it was found that they tended to be young, between the ages of 18 and 30 years. Some embezzlers were older. SRI asserted that perpetrators were highly motivated, intelligent, and personable and were considered good workers. Many of them were considered to be overqualified for their jobs and none entered their employment with the idea of doing anything illegal. Most violators, SRI found, had been employed for several years and had no history of job problems prior to initiation of their crimes. Accordingly, computer criminals, SRI said, were not "the typical white-collar criminal"; nor should they be considered "professional criminals." On the contrary, SRI said, the computer violator seemed to be a person who, for reasons of a personal nature, felt that crime by computer would reap short-term benefits or solve personal problems. The staff of the Senate Government Operations Committee interpreted this last trait in the SRI computer criminal profile to mean that violators, in many instances, turned to criminal acts to pay off financial debts.

SRI went on to say that, in its computer criminal profile, violators rationalized their acts by telling themselves that they were harming no one in particular and that if anyone, or anything, actually suffered losses it was persons who were rich enough—or institutions that were wealthy enough—to absorb such losses without serious difficulty.

"This would probably be particularly true of Federal civil service employees who see the Government as a bottomless pit of financial resources, quite removed from assets directly owned by people," SRI said. Moreover, While only three of the violators cited unhappiness on the job as being the primary motive for their criminal acts, most of them said disgruntlement at work did make them more inclined to commit the crime.

In a revelation which has special meaning to developing better crime control methods in computer operations, the 18 violators said they staked out their schemes by making an assessment of the audit systems in use at their given facility. The violators usually discovered they could defraud their employers by circumventing those same audit systems, once the systems were known to them. The computer criminals noted that audit systems rarely changed. "Therefore," SRI said, "it was simple to predict the auditors' activities and avoid discovery of the acts by the auditors."

SRI's report pointed to other traits of computer criminals as well. For one thing, the report said, violators were not especially sophisticated in the methods they used to compromise computer systems. They tended to perpetrate their crimes within their own work environments, and they were usually able to commit their crimes due to the fact that their supervisors trusted them within their work environment.

Similarly, SRI said, computer criminals who implemented more sophisticated tactics in attacking systems were frequently not primarily driven by the desire for financial gain—but instead, were inclined to challenge the computer ~~to~~ see if they could, indeed, compromise it. SRI said:

> The more sophisticated methods for compromising computers . . . tend to occur among the reported cases that have been perpetrated among students in educational environments (31 cases). These tend to be more malicious mischief rather than to result in serious loss. There is some concern that students in data processing environments in universities have come to look on the computer as a game-playing device and do not treat it with professional respect that a powerful tool deserves. These students may leave universities and go into their occupations carrying this game-playing concept with them, which results in an increasing number of computer abuse cases.

In his book, "Crime By Computer," Donn B. Parker assessed the potential risk inherent in the attitude of some computer personnel who see the highly sophisticated computer as not only a machine that can do lots of work quickly—but also as a challenge to be confronted and then conquered.

Parker wrote:

> A general characteristic of computer programers is their fascination with challenges and desire to accept them. In fact, they face the great challenge of making computer systems do their bidding day in and day out. Telling a [computer] programer that a computer system is safe from penetration is like waving a red flag in front of a bull. The challenge of an unauthorized act overshadows the question of morality.

> The idea that an abusive act is merely an innocuous game with the computer is often accepted in EDP (electronic data processing). Computer science students in universities, the so-called systems hackers, make a game out of attempting to compromise the campus computer system. Sophisticated compromises of campus computers abound. The idea of imparting to students the concept that the computer is an important, powerful tool upon which our livelihood and safety of society depends is almost nonexistent in universities. Although professional business ethics are passed from professor to student in university business schools, the same is not true of computer science departments.

A description of what Parker termed the "systems hackers" was given by Dr. Joseph Weizenbaum, a professor of computer science at the Massachusetts Institute of Technology. In his book, "Computer Power and Human Reason" (W. H. Freeman and Co., 1976), Professor Weizenbaum wrote:

> Wherever computer centers have become established . . . bright young men of disheveled appearance, often with sunken glowing eyes, can be seen sitting at computer consoles, their arms tensed and waiting to fire their fingers, already poised to strike, at the buttons and keys on which their attention seems to be as riveted as a gambler's on the rolling dice. When not so transfixed, they often sit on tables strewn with computer printouts over which they pore like possessed students of a cabalistic text. They work until they nearly drop, 20, 30 hours at a time. Their food, if they arrange it, is brought to them: coffee, cokes, sandwiches. If possible, they sleep on cots near the computer. But only for a few hours—then back to the console or the printouts. Their rumpled clothes, their unwashed and unshaven faces, and their uncombed hair all testify that they are oblivious to their bodies and to the world in which they move. . . . These are the computer bums, compulsive programers, . . . distinguished from a merely dedicated, hardworking professional programer . . .
>
> The compulsive programer is usually a superb technician. . . . He is often tolerated around computer centers because . . . he can write small subsystems quickly; that is, in one or two sessions of, say, 20 hours each. . . . His position is rather like that of a bank employee who doesn't do much for the bank, but who is kept on because only he knows the combination to the safe . . .

Independent inquiry by the committee staff revealed that some Government personnel, particularly in the area of national defense, are troubled by the possibility that persons Parker referred to as "systems hackers" and as Professor Weizenbaum termed "compulsive programers" could cause problems of varying degrees of seriousness to Federal computer programs. Whether through the desire to make mischief or to create genuine damage, such persons, working in an academic environment where Federal contracts are also being executed, could, it is feared, compromise, gain unauthorized access to, surreptitiously alter or otherwise render ineffective computer systems supporting Government programs.

IV. PERSONNEL AND PHYSICAL SECURITY IN COMPUTER PROGRAMS

The committee staff could not determine if any agency in the executive branch had the specific duty to assure that the Government's computer personnel security policies are effective and fair. However, it was established that the National Bureau of Standards does have a significant role to play in this regard.

The National Bureau of Standards (NBS), headquartered in Gaithersburg, Md., is part of the Department of Commerce. The NBS, according to the U.S. Government Manual 1976/1977, has the goal of strengthening and advancing the Nation's science and technology to promote their effective application for public benefit. NBS provides a national system for physical measurement. The Bureau also provides services to improve the use of materials and the application of technology, including the computer sciences and technology.

Located within NBS is the Institute for Computer Sciences and Technology. The Institute conducts research and provides technical services designed to aid Government agencies in the selection, purchase and effective use of automatic data processing (ADP) equipment. NBS has responsibility to develop standards for ADP equipment, techniques and computer languages. The Institute for Computer Sciences and Technology develops these Federal standards which NBS then issues under the name of Federal Information Processing Standards (FIPS).

FIPS–31

For the purposes of this preliminary staff investigation into computer security, the most significant Federal Information Processing Standard is Publication 31—referred to as FIPS–31—which the National Bureau of Standards issued in June of 1974. FIPS–31 has the title, "Guidelines for Automatic Data Processing Physical Security and Risk Management." The NBS FIPS–31 includes details on how to protect against such threats as loss from fire, flood, sabotage and theft and how to decide what security measures to provide in what circumstances. FIPS–31 also advocates a concept of risk management; that is, as the General Accounting Office defines computer risk management, "making a formalized assessment of the resources to be protected versus the cost to protect them and whether the cost involved is worth it."

The General Accounting Office, in its May 10, 1976 report on computer security, said the FIPS–31 publication "should go a long way in aiding Federal officials in making and justifying essential security decisions." While FIPS–31 had been out such a short time that GAO auditors could not evaluate its effectiveness at the time they wrote their report, GAO did cite shortcomings in FIPS–31.

First of all, GAO said, FIPS–31 is not a set of standards which each agency must adhere to; but is, instead a series of voluntary "guidelines." In addition to not being mandatory, GAO said, the guidelines apply only to new installations or those embarked on an effort to improve their computer systems. "Moreover," the GAO report said, "the guidelines do not and could not be expected to assign responsibility for this function to an appropriate management official."

This last point put forward by GAO—the concept of an "appropriate management official"—was one of the major recommendations for corrective action in Federal computer programs. Such an official would have a background in both automatic data processing and in security work, GAO said, stressing that every Federal installation that uses computers should have such an official. Only then, GAO said, could the successful implementation of FIPS-31 be achieved.

GAO investigators were also troubled by the fact that the Office of Management and Budget (OMB) had not firmly backed FIPS-31 through a policy statement in support of the guidelines. In fact, GAO said, OMB's response to this criticism was to assert that it was not necessary to issue any further policy directives regarding FIPS-31. OMB felt it would have been more appropriate for GAO to have directed its recommendations to improvements needed in FIPS-31 and to the conditions found at the computer installations visited, the GAO report said.

The GAO report went on to say Public Law 89-306—the first comprehensive legislative act regarding computer management—assigned the Government-wide responsibilities for computer management to OMB. The Department of Commerce was made responsible for technical standards, GAO said, adding that current Government-wide automatic data processing (ADP) policies "do not adequately cover ways or concepts to protect this annual multibillion dollar activity which permeates most facets of government operations."

GAO said that according to James T. Lynn, the Director of OMB, Public Law 89-306 and Executive Order 11717 of May 9, 1973 the National Bureau of Standards has the responsibility and authority to develop, coordinate, and issue appropriate uniform ADP technical standards. But, GAO pointed out, technical security standards are not the same as computer security guidelines. "Had NBS issued ADP security technical standards," GAO investigators said, "we would have addressed our recommendations . . . to NBS. The NBS guidelines [FIPS-31], however, were issued as a reference document—not as an ADP technical standard."

The GAO report did not recommend that FIPS-31 be immediately imposed through Federal programs—but GAO did assert that there should be some degree of insistence from OMB that the NBS guidelines be exercised. ". . . the guidelines are still in the developing stages and must be refined further," GAO said. "However, unless the agencies use the guidelines it will be difficult to gain the experience needed to improve them."

The GAO report added:

> . . . the NBS guidelines [FIPS-31] are not a rigid, unflexible set of rules. They instead provide matters to be considered in arriving at an intelligent, cost-effective approach to matching risk against severity of possible loss.

They are meant to be applied selectively. We believe they are a good vehicle to initiate Federal agencies in the use of sound physical security practices and risk management advocated in our report. Finally, we believe that the importance of good security for ADP facilities outweighs any further delay for achieving more perfect guidelines.

HISTORY OF NBS IN COMPUTER FIELD

Computer standards from the National Bureau of Standards are first developed in the Bureau's Institute for Computer Sciences and Technology. The Director of the Institute is Dr. Ruth M. Davis, Ph. D. As chairman of the Government Operations Committee, Senator Abe Ribicoff of Connecticut wrote to Dr. Davis July 19, 1976 for information relating to the role of NBS in Federal computer programs. Dr. Davis replied in a letter of September 2, 1976.

Dr. Davis said in her letter that Public Law 89-306, enacted October 30, 1965, and commonly referred to as the "Brooks Act," spelled out responsibilities for the Commerce Department in Federal computer applications. These responsibilities were then delegated by the Department to NBS.

The purpose of Public Law 89-306 was to "provide for the economic and efficient purchase, lease, maintenance, operation and utilization of automatic data processing equipment by Federal departments and agencies." Under the law, according to Dr. Davis, the Commerce Department, specifically the Department's National Bureau of Standards, was given these scientific and technical duties:

> To provide scientific and technological advisory services relating to automatic data processing and related systems to Federal agencies and the Administrator, General Services Administration,
>
> To make appropriate recommendations to the President relating to the establishment of uniform Federal automatic data processing standards, and
>
> To undertake necessary research in the sciences and technologies of automatic data processing, computer and related systems.

In her letter of September 2, 1976, to Senator Ribicoff, Dr. Davis cited a memorandum circulated throughout the Government by President Lyndon B. Johnson on computer technology. The memorandum, dated June 28, 1966, emphasized the need for heads of Federal agencies to make the best possible use of computer technology and said the National Bureau of Standards had responsibility "for the development of data processing standards and the provision of assistance to agencies in designing computer-based systems." President Johnson added, "I expect all agencies to cooperate fully with . . . the Department of Commerce . . . in accomplishing [this] objective."

On December 15, 1966, Phillip S. Hughes, the Acting Director of the Bureau of the Budget of the Executive Office of the President, sent Commerce Secretary John T. Connor a guidance paper asserting how NBS was to carry out its duties under Public Law 89-306. The policy guidance paper, Hughes wrote, was worked out by Bureau of the Budget personnel and Commerce Department officials.

The Bureau of the Budget, later to become, as presently constructed, the Office of Management and Budget, was to provide "fiscal and policy control" over the actions of the Commerce Department in computer operations, Hughes wrote. This fiscal and policy control was spelled out in section 111(g) of Public Law 89–306, Hughes said.

BOB Acting Director Hughes wrote:

> It is widely recognized that major hindrances to improving the use of ADP are the absence of: (a) standardization in character sets, input-output media, and interfaces which provide for compatible interchange of information and interoperation of systems and equipment; (b) standardization of computer programing languages; and (c) yardsticks for evaluating software and its effect upon the performance of the computer system. The Department [of Commerce] should concentrate on actions which will overcome these deficiencies.

Dr. Davis said that on May 9, 1973 President Richard M. Nixon issued Executive Order 11717. Dr. Davis said this order transferred to the Department of Commerce all functions being performed by the Office of Management and Budget (OMB)—formerly the Bureau of the Budget—having to do with the establishment of Govern ent-wide ADP standards. Executive Order 11717 transferred from OMB to Commerce and NBS "the function of approving standards on behalf of the President," Dr. Davis added. She said that Executive Order 11717 resulted in NBS receiving responsibility for the Federal data standards program which OMB had retained when it issued its 1966 policy guidance on implementation of Public Law 89–306.

Dr. Davis said that on July 1, 1975 the Office of Management and Budget issued OMB Circular A–108. This circular was entitled "Responsibilities for the Maintenance of Records by Federal Agencies." Dr. Davis said the circular assigned to the Commerce Department's National Bureau of Standards "responsibility for issuing standards and guidelines on computer and data security in accordance with OMB guidance relative to the Privacy Act of 1974."

CONFUSION OVER FIPS

In his letter of July 19, 1976, to Dr. Davis, Senator Ribicoff raised the issue of how effectively the NBS standards were being implemented throughout the Government.

Senator Ribicoff said in his letter that independent inquiry by the committee staff had developed information indicating that there was confusion and uncertainty in the executive branch owing to the lack of any compliance mechanism in the implementation of Federal information processing standards (FIPS) within the Federal Government. Senator Ribicoff said it was the committee staff's understanding that this situation had existed since the first FIPS standard was issued in 1968. It was the staff's further understanding that Public Law 89–306, which established the FIPS program, did not address the issue of compliance or enforcement and that none of the OMB policy guidance papers or executive orders since 1965 clarified the issue. Senator Ribicoff asked Dr. Davis to respond to the committee staff's findings.

Dr. Davis replied:

> The April 23, 1976 memorandum from the NBS Legal Advisor to the Assistant General Counsel for Science and Technology, Department of Commerce, sets out his summary of the present status regarding compliance mechanisms for Federal Information Processing Standards [FIPS] within the executive branch. It cites, for example, that the Brooks Act "does not address the issue of enforcement where there is a lack of compliance with ADP standards. Thus, the question that arises is whether the Secretary of Commerce has legal authority to effect compliance on a Government-wide basis."
>
> In June 1976, it was determined that the Secretary of Commerce under Executive Order 11717 of May 1973 may require agencies to report on the extent of their implementation of the FIPS. Prior to this determination NBS had taken only informal action to determine standards compliance. The first instance of this was a 1972 assessment to determine the significance and impact of ASCII (American Standard Code for Information Interchange) as a Federal standard. During this assessment, Federal agencies that participated on the task group were asked to provide implementation information. The effort was only partially successful due to the stated extensive costs for agencies to obtain this needed data.
>
> This first assessment of compliance could not realistically have been undertaken earlier. The ASCII standard, issued in 1968, was the first significant Federal information processing standard (FIPS). Full implementation of such a standard where costs are incurred by Federal agencies is assumed to require up to 5 years under the normal implementing procedures.

In his letter to Dr. Davis, Senator Ribicoff said:

> . . . the committee staff has found that since 1971 NBS has continually cited confusion surrounding the lack of an explicit compliance mechanism as a significant factor in the degradation of the credibility and effectiveness of the FIPS program, a deficiency which affects both NBS and the Commerce Department. What is the NBS response to that staff finding?

In her reply, Dr. Davis cited NBS Report 10608 of September 1971. The report is entitled "Brooks Bill Issue Study of the National Bureau of Standards." Dr. Davis said the report was written by NBS at the request of the Office of Management and Budget (OMB). Dr. Davis said OMB requested that the NBS report address this question: "What can be done to make the contribution of the NBS more effective in achieving greater efficiency and economy in Government ADP operations as envisioned in the Brooks bill—Public Law 89-306?"

Dr. Davis went on to say:

> In that report, page III, 9-10, NBS recommended a reporting system whereby agencies would report on the

> extent of standards implementation for each individual system and installation. The report continued by recommending that each Federal agency assume responsibility for standards implementation by its constituent organizations and submit reports on a regular basis to the Office of Management and Budget. NBS would serve as an appeal mechanism for Federal agencies where technical probelms were cited as a basis for requesting waivers. NBS stated that such a standards reporting system should provide sufficient information for NBS to determine if standards are responsive to needs and what modifications or additional standards are needed. NBS, in 1971, offered to assist OMB in developing the standards reporting system.
>
> Since 1971 NBS has taken other actions to measure compliance with Federal ADP standards. In this regard, there are two types of measurements for determining compliance with standards. One is technical; the other is managerial. As technical measurements, NBS has developed tests for measuring compliance with magnetic media standards and these have been implemented by GSA [General Service Administration] in testing computer tapes acquired for Federal use. In the programing language area, NBS has arranged for the testing of COBOL compilers in compliance with the standard. This testing is performed by the Navy through a joint agreement between NBS and DOD [Department of Defense]. Twenty-seven compilers and compiler versions have been tested and only two of these were determined to have no deviations from the standard. Other technical compliance tests are being developed for computer security and other programing languages. Similar compliance tests have been developed for the FORTRAN and BASIC programing language standards soon to be adopted.
>
> Managerial compliance involves determining the extent that standards are or are not being implemented by Federal agencies and taking appropriate measures to assure adherence with approved standards. As first stated in the NBS Report 10608, of September 1971, there still needs to be, in my view, a centralized reporting system on standards implementation that would provide information on: The extent that standards have been implemented; agencies' implementation plans; copies of agency implementation directives for standards; problems encountered in implementing standards; actions on waivers for standards; and additional standards that are needed by agencies in their ADP operations and procurements.

In his letter, Senator Ribicoff said it was the Government Operations Committee staff's finding that OMB in 1976 advised NBS on an informal basis that Executive Order 11717 of May 9, 1973, gives the Commerce Department all needed authority to enforce compliance or use, as appropriate, with FIPS standards and guidelines. However, Senator Ribicoff said, the committee staff found that no formal assurance of such authority had been given to NBS. In turn, Senator

Ribicoff said, it is the staff's understanding that NBS, in a memorandum of April 23, 1976, asked the Commerce Department's General Counsel to determine whether the Secretary of Commerce has the legal authority which OMB, on an informal basis, reportedly said it had. Senator Ribicoff asked Dr. Davis for the NBS response to the committee staff's sssertions.

Dr. Davis replied:

> The committee staff's findings based on its preliminary inquiry are correct.

She added:

> Since the Department of Commerce is still in the process of undertaking to determine the legal authorities of the Secretary to require compliance with the FIPS . . . we are unable at this time to provide you with a response from the Department on this matter. However . . . I have been informed that the Department, under Executive Order 11717, may require agencies to report on the extent of their implementation of the FIPS.

Senator Ribicoff advised Dr. Davis of an additional committee staff finding. It was that any Federal program intended to meet legislative requirements, such as those of the Privacy Act of 1974, needs an accompanying compliance and enforcement mechanism. Dr. Davis was asked if she agreed with the staff finding. She said she did agree, explaining, "With respect to standards, I have stated in previous testimony to Congress that there should be compliance mechanisms."

Dr. Davis also said on this point:

> In section 6 of the Privacy Act assigned responsibility to OMB to (1) develop guidelines for the use of agencies in implementing the act and (2) provide continuing assistance to and oversight of this implementation. In circular A-108, OMB assigned responsibility to the Secretary of Commerce (NBS) as follows: "The Secretary of Commerce shall, consistent with guidelines issued by OMB, issue standards and guidelines on computer and data security."

FIPS-31 "GUIDELINES"

Already cited in this staff study was the Federal information processing standards (FIPS) publication 31, issued in June of 1974, on physical security in Federal computer programs. Senator Ribicoff, in his letter to Dr. Davis, asked why NBS had referred to the FIPS-31 as a set of guidelines and why this publication was not characterized as a standard. Senator Ribicoff asked Dr. Davis to differentiate between guidelines and standards. The staff had information indicating that FIPS-31 was the first time NBS had characterized a FIPS publication as a set of guidelines.

Dr. Davis said a standard, as defined at NBS, is a "Prescribed set of conditions and requirements, of general or broad application, established by authority of agreement, to be satisfied by a material, product, process, procedure, convention, test method; and/or the physical, functional, performance, or conformance characteristic thereof."

Dr. Davis went on to say that she had introduced the use of guidelines in the FIPS program in 1973.

She said:

> . . . I view guidelines as a means of resolving problems where there is a recognized Governmentwide need for uniformity in physical, functional, performance, or conformance characteristics in automated information processing technical processes and (1) where there is inadequate costing data to justify imposing a standard which may be impossible for agencies to implement within existing budgets or (2) when there is inadequate experience to justify imposition of a supposedly mandatory standard. In this sense, guidelines often serve as an interim step toward gaining the experience or compiling the data needed for the issuance of a formal standard. I know of no formally approved definition of "guideline" for use in Federal standardization activities.
>
> The principal difference between FIPS standards and FIPS guidelines is probably best explicitly described by the difference in the implementation requirements which accompany each FIPS standard and guideline. For standards, an implementation schedule and waiver procedure is specified. For FIPS guidelines there is no required implementation schedule or waiver procedure.

Senator Ribicoff called to Dr. Davis' attention an observation made by the General Accounting Office in its computer security report in which GAO said that "Unless the agencies use the guidelines, it will be difficult to gain the experience needed to improve them."

Furthermore, it was the committee staff's view, Senator Ribicoff said, that in those instances in which guidelines have been issued, it is particularly important to clarify where the responsibility lies for requesting Federal agencies to use them.

Dr. Davis said:

> I believe that there needs to be a clarification of the use of FIPS guidelines and agreement by Federal agencies as to their purpose and utility. I have asked (as of Aug. 4, 1976) the Chairman of the Federal Information Processing Standards Coordinating and Advisory Committee (FIPSCAC), which advises and assists the Secretary of Commerce in carrying out his Public Law 89-306 responsibilities, to review and make recommendations on this policy issue. GSA has a membership on FIPSCAC.

FIPS-31 on Personnel Security

Public Law 89-306, the Brooks Act, directed that the National Bureau of Standards (NBS) in the Commerce Department was to establish standards for automatic data processing (ADP) operations in Federal programs.

In the field of security, these standards were issued by NBS in June of 1974 in the form of a Federal Information Processing Standards Publication 31, or, as it is known by the acronym, FIPS Pub 31.

The title of FIPS Pub 31 is "Guidelines for Automatic Data Processing, Physical Security and Risk Management."

The document is 91 pages long and covers a broad range of computer security considerations, ranging from "Anticipating Natural Disasters," to "Security of Off-site ADP Facilities," to "Internal Audit of Physical Security." The team of computer experts from the General Accounting Office found the FIPS Pub 31 to be, in general, a constructive document but, GAO investigators note, it was only a set of "guidelines" and there was no compliance mechanism to insure its application throughout the executive branch. To executive branch spokesmen who said FIPS Pub 31 should not be made mandatory because it needed further refinement and evaluation after initial application, GAO's response was that FIPS Pub 31 could never be refined and evaluated if it was not tried out throughout the Government. In effect, GAO investigators asked, how can a system for computer security be tested and then improved if no agency is first of all required to test it?

This staff study will now summarize FIPS-31 as it relates to the primary interest of the Senate Government Operations staff's preliminary investigation; that is, computer security, with special focus on personnel security considerations.

In its chapter, "Physical Protection of ADP Facilities," FIPS-31 addresses itself to "the roles of people" and warns against the efforts of "common criminals," "activists," "espionage agents," and "vandals."

FIPS-31 says that, regarding common criminals, the main concern should be with the theft of Government property. Would a burglar be likely to think there is valuable property in the building? the FIPS-31 document asks, explaining that this might include theft of office machines, firearms, drugs, cash, personal possessions, or any other items subject to easy resale or useful for other criminal activities.

As for activists, FIPS-31 notes, the agency should determine whether its activities are perceived to be controversial. Could the installation be considered a desirable symbolic target which activists might wish to penetrate and thereby generate public attention for themselves?

The FIPS-31 document goes on to explain:

> An activist group forced entry at a Midwestern research laboratory's ADP facility with the intention of destroying magnetic tape data files for research projects of which the group disapproved. No employees were present at the time and the activists did not damage any of the hardware. A number of tapes were said to have been erased and punched cards were thrown on the floor. The group was not discovered during the break-in but revealed themselves at a press conference a few days later. The research laboratory is said to have increased its patrol force coverage and given consideration to intrusion detectors subsequent to the break-in. While damage was estimated to be no more than $100,000 this episode points up the importance of safeguarding an ADP facility against intrusion.

On the subject of espionage agents, FIPS-31 says that Federal computer installations should determine whether or not their facilities hold or process data which could be of value to an outsider prior to its public release concerning subjects such as economic activity, future allocation of Federal funds, or sensitive personal information.

If vandalism is prevalent in the area where the computer installation is located, Federal officials should know about it and—in the threat of vandalism, as in the threats of common criminals, activists, and espionage agents—they should insure that their ADP facilities are secure.

FIPS-31 asserts that Federal computer installations which require full-time guards should engage this kind of personnel through the Federal Protective Service of the General Services Administration (GSA) or "guards furnished by a private company under contract."

Another chapter of FIPS-31 is devoted to "Internal Controls." In this chapter, the issue of computer personnel security is addressed.

FIPS-31 asserts:

> People are undoubtedly the most important part of the ADP facility, and no ADP facility can function without a trained staff dedicated to achieving the mission of the agency. Personnel controls should reflect the need for careful selection of mature, trustworthy people for sensitive positions, the importance of providing adequate training to assume competent performance of ADP duties, and the value of good supervision in achieving a high level of motivation.
>
> The selection of personnel routinely includes an effort to determine that the candidate is qualified by training, talent, and experience to perform the duties to be assigned. In addition to this determination of job skills, the selection for sensitive ADP positions should also verify the trustworthiness of the candidate for sensitive positions by appropriate prehire screening. Several levels of screening are available and, of course, both effectiveness and cost increase as the depth of the investigation increases. Therefore. the level of screening used should reflect the relative sensitivity of each position. Each ADP facility must define for itself its sensitive positions; generally these will include computer operations, data control, management, auditing, and programing (including acceptance testing and maintenance) of critical applications and systems. The risk analysis for fraud will usually identify critical interface points. Wherever a critical interface involves a single individual, the position is probably sensitive. This is especially true for hidden interfaces in which checks and balances are missing; for example, a single programer for creating, testing, debugging and installing a critical program. The most sensitive position is often that of the system programer; a qualified practitioner of operating system maintenance can do more damage with less chance of being caught than almost any other person involved with data processing.
>
> Each Federal department or independent agency has established regulations and procedures for designating one or more levels of position sensitivity and the screening

applied to each sensitivity level. The ADP security planner should establish the appropriate level to apply to each ADP facility position.

CIVIL SERVICE LETTER OF SEPTEMBER 15, 1976

Personnel security was the subject of a letter Senator Ribicoff wrote to Civil Service Commissioner Robert E. Hampton on August 27, 1976. Senator Ribicoff wanted to know, for example, the Civil Service Commission's view of FIPS–31.

In a reply of September 15, 1976, Civil Service Commissioner Hampton said the Commission "did not formally evaluate FIPS PUB 31." But, he said, Commission officials familiar with computer operations felt the document "is a valuable study with sound recommendations."

Hampton said the Commission had reviewed the committee print issued on June 21, 1976, by the Senate Government Operations Committee entitled, "Problems Associated with Computer Technology in Federal Programs and Private Industry." Hampton said the committee print had lead him to believe that "most Federal positions connected with ADP operations should be designated critical sensitive, requiring a preappointment full field investigation."

Hampton went on to say that the Commission's Bureau of Personnel Investigations "wholeheartedly endorses" the idea that preemployment investigations be required for persons selected for "sensitive" ADP positions.

Hampton added:

> The most sophisticated physical security system, without a correspondingly tight personnel security program, provides only a false sense of security.

In addition, Hampton said, the language in FIPS–31 asserting that ADP personnel should undergo "appropriate preemployment screening" had been interpreted by the Civil Service Commission "to mean a preappointment (background) investigation to establish the selectee's reputation with respect to honesty, integrity and trustworthiness."

While Civil Service Commissioner Hampton expressed the opinion that preappointment background investigations should be conducted on persons about to be hired by Federal agencies for work in the ADP field and that most positions in this area should be designated "critical sensitive," it was a finding of the Committee staff that, as of September 15, 1976, the date of Hampton's letter, Federal positions in the ADP field has not been designated "critical sensitive"; accordingly, no full field background investigations were required.

HOUSE COMMITTEE HEARINGS

In its evaluation of computer personnel security policies in Federal programs, the Senate Government Operations Committee preliminary staff investigation found information indicating that security procedures needed to be improved. Other aspects of automatic data processing (ADP) in Federal programs were also found to be in need of improvement. One demonstration of inadequacies was seen in an inquiry and hearings conducted in the House of Representatives.

The Subcommittee on Legislation and National Security, chaired by Congressman Jack Brooks of Texas, is part of the full House Committee on Government Operations, also chaired by Congressman Brooks. On June 28 and 29 and July 1, 1976, the subcommittee held hearings on the effectiveness of the executive branch in carrying out the first and most comprehensive legislative act affecting computers in Federal programs, Public Law 89–306. Commonly known as the Brooks Act, Public Law 89–306 was adopted in 1965 and the purpose of the House hearings was to evaluate how the Government had administered the measure over the last decade.

In a report dated October 1, 1976 and issued by the full House Committee, members of the committee said the Brooks Act had been neither administered nor implemented in accordance with the intentions of Congress.

The report, entitled "Administration of Public Law 89–306, Procurement of ADP Resources by the Federal Government," was especially critical of the three "lead" agencies which were to set, manage and implement policy in computer operations in Federal programs. The "lead" agencies are the Office of Management and Budget (OMB), the General Services Administration (GSA) and the National Bureau of Standards (NBS) in the Commerce Department.

The House committee said GSA had repeatedly authorized noncompetitive procurements which were not adequately justified; GSA had failed to enforce regulations and restrictions in ADP procurement authority delegated to user agencies; GSA had not provided adequate management guidance to user agencies; OMB had failed to establish concise, clearcut policy; OMB had not provided adequate direction in the enforcement of those policies it had established; NBS had failed to provide necessary hardware and software standards; Federal user agencies had consistently failed to cooperate with GSA; and Federal user agencies had shown a general reluctance to adhere to the purpose and intent of the Brooks Act.

The report pointed out that under the Brooks Act, GSA has the authority for procuring ADP resources required by Federal user agencies. GSA, the House report said, may either buy those ADP requirements which a user agency specifies or delegate to an agency authority to procure under restrictions and conditions specified by GSA.

The Brooks Act does not permit GSA to impair or interfere with an agency's determination of its requirement, the House report said, adding, however, that this did not prevent GSA from deciding the best means for a given agency to fulfill its computer requirements. The House committee report noted that any dispute between GSA and a user agency was to be resolved by OMB.

House committee members said they had surveyed Government procurement practices for fiscal year 1975 and found that only 36 percent of the systems required were procured in a fully competitive manner. The report also pointed out that this percentage did not include a large number of noncompetitive delegations granted by GSA under Temporary Regulation E–32, relating to renewals of leased equipment rented under the ADP schedule. If these procurements had been included, the House report said, the percentage of competitive procurements would have been even lower.

The House report said the remaining procurements in the computer field were noncompetitive—"sole source, make and model, brand name or equal." The committee members said this low percentage of competitive procurements was inconsistent with the goals and objectives of the Brooks Act and reflected a decline in the level of competition over an 8-year period. What the House Members found particularly disturbing, they said, was that noncompetitive procurements are more costly to the Government than are competitive procurements. GSA acknowledged this fact in testimony before the the House committee. The House report said that, according to GSA, since enactment of Public Law 89-306, more than $681 million in cost avoidance had been achieved in 302 competitive ADP contracts.

The House report said that the Brooks Act had stimulated a greater participation in the Government market by ADP manufacturers than in the commercial market. Seventy percent of the commercial computer market is dominated by one firm, the House report said, but that same firm controls only about 30 percent of the Government market. "While the Brooks Act can justifiably take credit for this, these statistics do not represent true competition in the sense that they do not reflect whether competition occurred in any specific procurement," the House report said.

In its criticism of the manner in which the executive branch was administering the Brooks Act, the House Government Operations Committee was especially harsh in its comments about GSA's relationship with user agencies such as the Veterans' Administration, the Social Security Administration, and the Departments of Interior, Agriculture, Commerce, Transportation and Health, Education, and Welfare.

The House report said, for example, that the General Accounting Office had documented several cases in which GSA granted procurement delegations which had not been fully justified by user agencies. Among these, the report said, were procurement requests by the Department of Agriculture, the VA, and the Social Security Administration.

Several reasons existed for GSA's actions, the House report said, foremost among them being that GSA lacks the resources to examine in depth an agency's justification for a noncompetitive procurement. The House report said that to conduct an adequate in-depth review of a justification for a major ADP system would require the expenditure of hundreds of man-hours by technically qualified personnel. Generally, the House report said, GSA lacks sufficient manpower to devote that amount of time to such reviews. The Federal Computer Performance Evaluation and Simulation Center (FEDSIM) does possess the capability to perform such services, the House Committee said, but the Center's resources are so limited that it is unable to provide a significant degree of timely assistance in this area.

The House Committee report then went on to make, in a significantly strong indictment of procurement practices in the executive branch, this criticism of GSA and GSA's relationship with other executive agencies:

> . . . GSA, on occasion, appears to grant a user agency a delegation of procurement authority because of the latter's prestige or dominance in the bureaucratic structure of Government. In essence, this prestige or dominance permits an

> agency to exercise influence over another agency without taking any apparent overt action. This influence stems from the mission of the agency and the support it can garner from the higher levels of Government. GSA, unfortunately, ranks below many other agencies in the world of bureaucracy. As a consequence, it is unable, standing alone, to resist pressures from a more dominant source if such source signals GSA that it intends to exert pressure concerning a particular request.

The House report said there had been occasions when user agencies had refused to cooperate with GSA when GSA sought fuller justification for noncompetitive procurement requests. In recent months, the House Members said, the Departments of Interior, Commerce, Transportation, and HEW had challenged GSA's authority to obtain additional documentation for procurement requests. These challenges, the House report said, were based on the section of the Brooks Act which prohibits GSA from questioning an agency's requirements. The House report said the validity of these challenges was without legal support under the law. The House Committee report pointed out that if an agency disagrees with GSA regarding justification for a particular procurement the Brooks Act provides that the dispute be brought to OMB for resolution. In the past, the House Members said, neither GSA nor the agencies had exercised this right to appeal to any extent.

The House report then noted:

> The committee is very disturbed over an apparently increasing trend of user agencies to interpret the law to suit their own purposes. Whether intentional or not, this type of behavior will have the effort of subverting the effectiveness of Public Law 89-306. If GSA were to be denied the right to require full documentation for ADP procurements, the objectives of fully competitive procurements under the act would be effectively destroyed. Federal agencies strongly resisted enactment of the Brooks Act. Since passage, they have shown little willingness to comply voluntarily with the law. The low level of fully competitive procurements further illustrates their noncooperative state of mind. Either user agencies must learn to comply with the full thrust of the act or OMB must take all necessary action to make them do so. In particular, OMB must make it clear to every user agency that its right to determine its own ADP requirements under the act does not include the right to dictate a special brand name of equipment as its requirements or refuse to supply GSA with appropriate feasibility studies. In addition, GSA must be given the resources to perform adequate reviews of users agencies' procurement justifications.
>
> GSA, in turn, must take a more aggressive position when dealing with user agencies. Being fully cognizant of the bureaucratic facts of life, however, it has to be realized that GSA will not be able to assume this role unless OMB fully supports it.
>
> The manner in which the Brooks Act is being administered is unacceptable. If this continues, the act's effectiveness will become seriously jeopardized at a cost of millions of dollars to the taxpayers.

Of special interest to the Senate Government Operations Committee in its preliminary staff inquiry concerning computer security problems in Federal programs was a finding made by the House committee regarding the role of the National Bureau of Standards in developing and promulgating standards for ADP applications.

The House committee urged the executive branch to initiate as soon as possible a program to enable NBS to develop meaningful standards for computer hardware and software.

Noting that under the Brooks Act and Executive Order 11717 NBS is charged with responsibility for developing ADP standards, the House report asserted that the General Accounting Office had "expressed serious concern about the lack of progress being made by NBS in the development of standards."

The House committee report said NBS had only developed to a limited extent standards necessary to fully implement the Brooks Act. The report said that NBS spokesmen had acknowledged that lack of standards seriously impeded effective competition in the procurement area. The report also said that testimony at the House hearings from the Computer Industry Association indicated that NBS had developed no meaningful hardware standards and only a relatively few software standards. GSA made the same charge, the House report said.

The House report went on to say that even in those cases in which standards have been adopted, their implementation has not been effectively enforced. NBS said it had no data on agency compliance with standards and that enforcement of standards resides in each individual agency, the House Members asserted.

GSA, the House report said, has incorporated most Federal standards into its procurement regulations but GSA has made little or no effort to see that they are complied with.

The House report said OMB last exercised its policy guidance role in this area in 1966—soon after passage of the Brooks Act—when it issued policy guidelines to NBS. Since that time, the report said, OMB has neither updated these guidelines nor taken action to see that they are followed. The report said that even if standards are adopted in the future such development will be of little value unless an effective means of enforcement is developed.

The House report said that NBS indicated that centralizing responsibility will improve compliance. But, the report said, NBS spokesmen say NBS is not an appropriate agency to enforce compliance. "In consequence," the House report concluded, "OMB must establish procedures for the effective enforcement of ADP standards and designate GSA as the agency responsible for enforcing compliance with such standards."

While the House Government Operations Committee report focused primarily on procurement and utilization of ADP resources, the report's conclusions—particularly as they relate to NBS standards and a compliance mechanism to enforce them—have relevance to computer security. It was the view of the staff of the Senate Government Operations Committee that just as there is no compliance mechanism to enforce procurement and utilization standards; neither is there a compliance mechanism to enforce personnel security, crime control, and plant security standards in ADP Federal programs.

GSA's Role in Computer Security

Senator Ribicoff wrote to Jack Eckerd, Administrator of the General Services Administration, July 9 and July 29, 1976, in connection with the Senate Government Operations Committee's preliminary staff investigation of problems associated with computer technology in Federal programs and private industry. In addition, committee staff met with GSA officials, including Theodore D. Puckorius, Commissioner for Automated Data and Telecommunications Service, in Puckorius' office on August 11, 1976. On November 9, 1976, Administrator Eckerd submitted a 112-page statement to the committee. In his letter of transmittal to Senator Ribicoff, Administrator Eckerd noted that the response was in "draft" form but added that, "While a final version of material submitted for the record might differ in minor respects, the substance of GSA's responses would remain the same." Accordingly, this staff study will represent GSA's views on computer considerations as Mr. Eckerd represented them in his "draft" response.

Administrator Eckerd said Public Law 89-306, the Brooks Act, authorizes and directs GSA to coordinate and provide for the economic and efficient purchase, lease, and maintenance of ADP equipment by Federal agencies. However, he noted, GSA cannot question any agency's computer requirements. Eckerd said the Brooks Act prohibits GSA from impairing or interfering with the decision by any executive branch agency as to what its ADP needs are. "This is significant," Eckerd said, "because unduly restrictive requirement statements may cause industry to propose less than the best solution to Government problems."

Public Law 89-306 gives GSA no specific Government-wide responsibility for computer security, Eckerd said. But, he added, GSA does have certain Government-wide responsibilities which relate to computer security. Those responsibilities, he said, have to do with protection of personal data and with protecting Government buildings.

Regarding personal data, Eckerd said, the Office of Management and Budget (OMB), in its promulgation of instructions for administration of the Privacy Act of 1974, directed GSA to assure that procurement policies were such that the Privacy Act could be carried out. However, Eckerd said, neither the Privacy Act nor GSA's responsibility stemming from that act was directly concerned with the broader issue of computer security.

On the subject of public buildings security, Eckerd said GSA has responsibility to provide government-wide policy guidance and assistance to agencies as they seek to secure their installations. Again, however, as Eckerd pointed out, GSA's duties as they relate to securing public buildings are not directly concerned with computer facilities, but rather with all Federal installations. "In summary," Eckerd said, "GSA would like to emphasize that the Administrator of General Services does not have any specific government-wide responsibilities regarding computer security. Moreover, GSA is not aware of any statutes or executive orders which impose either government-wide or specific agency-level responsibilities for computer security."

Eckerd said, Public Law 89-306, the Brooks Act, did not delegate any specific computer security responsibilities to GSA.

He explained:

> . . . the act is silent on this subject. It is GSA's position that computer security is one facet of an agency's ADP requirement and, as such, its determination is the responsibility of individual agencies. Beyond providing for the security of its own internal ADP operations, GSA can currently exercise authority in computer security matters only in those cases where GSA is contracting with vendors for provisions of ADP services to other agencies, or where an agency attempts to specify computer security requirements in such a way as to unduly restrict competition.

Eckerd addressed his comments to GSA's relationship with OMB and the National Bureau of Standards (NBS) as together they seek to administer the Brooks Act. OMB is responsible for policy and fiscal control aspects of ADP management while NBS is charged with developing technical standards or "technical guidelines," Eckerd said.

In the development and promulgation of operating policies and procedures, and in the establishment of programs aimed at achieving more efficient acquisition, management and use of computers, GSA receives overall policy direction and fiscal control from OMB, Eckerd said. As for technical ADP standards and guidelines, Eckerd said, these are to be provided by NBS. "For example," Eckerd said, "in the computer security area GSA personnel are participating in efforts designed to produce computer security inspection guidance for Federal managers, to produce the necessary methods and procedures needed for adequately specifying security requirements in ADP procurements, and to facilitate the implementation of the data encryption standard sponsored by NBS." This encryption standard is the preferred technique for safeguarding confidentiality of coded data transmitted over communications links, either by radio or by wires.

The initials ADTS stand for GSA's Automated Data and Telecommunications Service. ADTS, under the direction of GSA Commissioner Theodore D. Puckorius, has the responsibility for fulfilling the administration's duties assigned it by Public Law 89–306.

ADTS has the primary responsibility, under the Brooks Act, to lease, purchase and maintain computer equipment and software for Federal agencies. However, Administrator Eckerd said, the Brooks Act enables GSA—and, in turn, GSA's ADTS—to delegate this responsibility to the individual Federal agencies. This delegation of authority can be executed, under the Brooks Act, "to the extent necessary and desirable," Eckerd said.

Before delegating this authority to a specific Federal agency, GSA first of all requires that the specific agency submit a procurement request when the proposed expenditure exceeds an established amount, Eckerd said. GSA, through its ADTS (Automated Data and Telecommunications Service) then reviews the request to determine if it meets regulations, Eckerd said. If the request is found to be appropriate and in accordance with Federal regulations, Eckerd said, the request is granted.

This system whereby individual agencies must submit purchase, lease and maintenance contracts to GSA for approval, Eckerd said, provides certain assurances that appropriate practices will be followed by individual Federal agencies. Eckerd was of the opinion that this procedure, while not directly affecting ADP security precautions, does enable GSA to maintain a semblance of oversight in the computer security field.

Eckerd explained:

> . . . ADTS reviews such requests for conformance with established regulations, and makes a decision on whether to delegate procurement authority to the agency or to conduct the procurement. Naturally, this is an oversimplification of the agency procurement request process. Our intent is to point out that a program of procurement management exists. It includes provisions for enunciating appropriate operating policies and procedures, and effecting necessary oversight of agency ADP equipment and related services acquisitions. Though not presently directed at specific issues and concerns regarding computer security, it is emphasized that this government-wide management vehicle provides a basis for: (1) establishing appropriate computer security related operating policies and procedures for ADP procurement activities; (2) making the use of appropriate standards mandatory and the applicability of reasonable guidelines known; and (3) assuring necessary operational oversight of how agencies provide for computer security within agency ADP procurement activities.

The staff of the Senate Government Operations Committee interpreted Administrator Eckerd's observations about GSA's approval of Federal agencies' computer procurement, leases and management contracts to be at variance with the findings of the House Government Operations Committee. The House committee, as noted in the previous section of this staff study, found that in fiscal year 1975 only 36 percent of the systems required by the executive branch agencies were procured in a fully competitive manner. The House report said that GSA should be given the resources to perform adequate reviews of user agencies' procurement justifications. In turn, the House committee said, GSA should take a more aggressive position when dealing with executive branch agencies. "Being fully cognizant of the bureaucratic facts of life, however," the House report said, "it has to be realized that GSA will not be able to assume this new role unless OMB fully supports it."

In their August 11, 1976, meeting with GSA officials, committee investigators raised the issue of the percentage of ADP hardware and software contracts which might have been awarded not in accordance with requirements as spelled out in the Brooks Act. The Senate committee staff said it had information that as much as 70 percent of these ADP contracts were awarded "illegally."

Eckerd's response to this assertion, as articulated in his November 9, 1976, statement to the committee, was as follows:

> While there have been some deviations from the intent of procurement regulations, particularly with respect to the requirement for full and free competition, it is doubtful that

> these deviations could properly be construed as being "illegal." In any event, we do not believe that the magnitude of this problem has been sufficient to warrant a costly study to determine the actual percentage in this category. Nevertheless, we monitor GAO reports and review procurement documentation relating to the acquisition of ADPE [automatic data processing equipment] and software for compliance with applicable directives. Although the enforcement, per se, of procurement regulators is not a responsibility of GSA, we do act to avoid delegations of procurement authority (DPA) in those instances where there is clear evidence that either the procurement regulations or the limitations of the DPA are being circumvented by the procuring activity. Also, we act to place specific restrictions on the use of GSA contracts for the acquisition of ADPE and software when contracts, such as our ADO schedules, are being abused.

In his statement for the Senate Government Operations Committee, GSA Administrator Jack Eckerd went on to discuss the NTS contract. NTS is the National Teleprocessing Services. Eckerd said NTS is a remote teleprocessing service that is available on a national scale to Government users having requirements for both interactive and batch modes of processing and the need to assess common data bases.

Eckerd said the General Services Administration manages NTS. He said services under NTS are provided by the Infonet Division of Computer Sciences Corporation, El Segundo, Calif. The contract with Infonet is governmentwide. The NTS services provided under the contract with Infonet have been successful, Eckerd said, as he explained:

> Based on the success of the NTS program, and more specifically on the costs avoided as a result of that program (savings of about $20 million in fiscal year 1975) ADTS initiated in fiscal year 1976 a new, expanded ADP teleprocessing services contract program: the teleprocessing services program (TSP).

Eckerd said the teleprocessing services program (TSP) will expand contractual coverage to meet widely diversified Government requirements now existing. He said the new program includes multiple award contracts and basic agreements to be used in separate competitive procurements.

Eckerd said:

> TSP when fully implemented will harness under a single program all Government contracting for ADP teleprocessing services. It is pointed out that this broadly based, government-wide program affords us an opportunity to uniformly provide for the computer security issues and concerns related to contracting for such services.

GSA Administrator Eckerd provided the Senate Government Operations Committee with a list of Federal Agencies which have used the Infonet system and with each Agency's net billings by Infonet for fiscal years 1974, 1975 and 1976. The Agencies and the billings of $200,000 or more reported by Administrator Eckerd are as follows:

	Fiscal year 1974	Fiscal year 1975	Fiscal year 1976
GSA	$3,331,627	$6,053,790	$5,929,225
Army	1,778,570	2,892,858	4,088,376
Navy	381,000	1,126,711	2,592,305
HEW	523,699	1,672,671	2,514,149
Agriculture	893,858	1,330,335	1,999,563
HUD	958,579	1,184,444	1,658,946
Postal Service		629,098	746,258
Defense Contract Audit Agency	371,367	710,852	726,358
ERDA			589,876
GAO		373,230	520,784
Department of Defense		211,458	519,119
SBA			428,058
American Revolutionary Bicentennial Administration		216,105	383,104
Interior Department	506,090	935,384	370,192
FEA			276,335
Commerce			231,034
NASA	450,268	313,712	230,932
Treasury			227,862
FTC			204,321
Civil Service Commission			201,535
OMB	234,579	377,001	
Other agencies	1,849,674	1,381,659	1,300,534
Total	11,279,496	19,409,308	25,718,866

Not listed by Administrator Eckerd as a Federal user of Infonet—perhaps because the billing was under $200,000—was Federal Prison Industries, Inc., an enterprise wholly owned by the U.S. Bureau of Prisons. Federal Prison Industries, Inc., manufactures and provides goods and services from the labor of inmates incarcerated in Federal penitentiaries. It was established by the Senate Government Operations Committee staff—and will be discussed further later in this staff study—that inmates incarcerated in the Federal Penitentiary at Leavenworth, Kans., were serving as programers for Government computer systems under contract to Federal Prison Industries, Inc. The inmates had access to the Infonet time-sharing ADP services.

The committee staff asked if the inmates' access to Infonet could compromise Infonet's security. "Not to any greater or lesser extent than access had by any other programers," Eckerd said. "Infonet is as reasonably secure as can be expected, given the requirements of the users employing it."

The committee staff expressed an interest in knowing how secure the Infonet system was. Administrator Eckerd said GSA's Office of Audits entered into a contract with the Stanford Research Institute, Menlo Park, Calif., to evaluate security procedures at Infonet. Eckerd said the Stanford Research Institute team, headed by Donn B. Parker, concluded, with GSA's Office of Audits, that "the data security features of Infonet were commensurate with the uses being made of the system." However, Eckerd said, "the evaluation did indicate opportunities to further enhance the data security of Infonet."

Administrator Eckerd said the SRI team, under the leadership of Donn B. Parker, was capable of making the evaluation of Infonet's security procedures. Parker, Eckerd said, "is a nationally recognized authority on computer crime and security of computer systems."

GSA was asked if, based on the SRI report, GSA was satisfied that Infonet is a secure system. Mr. Eckerd's reply was:

> Skilled persons can subvert the Infonet system, as can be done with every system now in existence. SRI concluded in its final report that "the overall security provided by Infonet meets and in some ways exceeds the low level of user demands and is consistent in many ways with current practice to the extent that has been determined through SRI experience."

Committee investigators who had read Parker's SRI report on Infonet security pointed out to GSA officials that their interpretation of the report was not the same as their own. Investigators said Parker had noted shortcomings in Infonet security procedures, particularly regarding the existence of unguarded passwords and unsecured terminal facilities.

Administrator Eckerd, in his statement for the committee refuted the staff's view, saying any shortcomings noted in Parker's report "reflect badly on the administrative and physical safeguards of individual user agencies, and these shortcomings and remedies for them have been brought to the agencies' attention. These are separate and distinct problems, however, from those of securing the Infonet system itself."

GSA was asked if Infonet was considered to be suitable for handling of defense classified material. "No," Eckerd said in his statement, adding that "user agencies have been so advised." In addition, Eckerd said, "To the best knowledge of GSA and of the contractor, no classified information is processed on Infonet."

In light of the committee staff's inquiry relating to the role of inmates at the Federal Penitentiary at Leavenworth, Kans., committee investigators asked GSA for specific figures on the amount of billings paid by the IRS to Infonet. Eckerd said the Infonet billings to IRS in fiscal year 1974 were $49,941; in 1975, $105,944; and in 1976, $147,886.

In this same regard, the committee asked about Infonet billings to the Department of Agriculture's Commodity Credit Corporation and the Agriculture Stabilization and Conservation Service. Both these Agriculture offices comprised the bulk of the computer programing work performed by the convicts at Leavenworth. Administrator Eckerd said that neither the Commodity Credit Corporation nor the Agriculture Stabilization and Conservation Service were "reflected in figures known to GSA." "If these organizations are obtaining services through another Infonet user," Eckerd said, "Infonet charges connected with those services will be reflected in billings made to the actual user."

The subject of Infonet and the use of its computer timesharing system by felons incarcerated at the Federal Penitentiary at Leavenworth led Senate committee investigators to inquire of GSA as to what was the nature of the services provided the prisoners by Infonet. The prisoner computer "programers use Infonet in support of system development activities," GSA Administrator Eckerd said in his statement for the committee.

In his letters to GSA, Senator Ribicoff asked about security procedures required of private firms which provide computer services for Federal agencies. This subject area is of significance because of an OMB circular, A–76, directing that Government contract its computer requirements with private firms whenever appropriate.

GSA Administrator Jack Eckerd said computer security was viewed at GSA as an element of each individual agency's ADP requirement. He said each agency is responsible for defining its own security requirements. Contractor firms then respond to the agency by preparing and presenting proposals for meeting these requirements, Eckerd said, adding that it is then up to the individual agency to determine if the private company can assure that appropriate security precautions will be met. "If, for example, a particular contractor's security procedures do not meet the agency's requirements, then this is a legitimate reason to consider that contractor nonresponsive and to select another contractor who does provide the needed level of security," Eckerd said.

Eckerd went on to say that GSA does not attempt to assure for other agencies the security or the integrity of private contractor operating systems and computer time-sharing programs.

Moreover, Eckerd said, GSA does not determine national defense or any other security levels required by agencies as they contract out computer services to private firms. Eckerd reiterated that it is GSA's position that computer security is the responsibility of the individual agency.

With reference to personal data, however, GSA does have a mission, Eckerd said. He explained that under OMB Circular No. A–108 GSA is held responsible for insuring that agencies comply with provisions of the Privacy Act of 1974 concerning reports on user systems and public notice of all systems of records. In that regard, Eckerd said, Federal agencies must now include in their requests to GSA for procurement and services information and certification relating to specific requirements protecting the privacy rights of individuals.

Senator Ribicoff asked if there were a role played by the National Bureau of Standards in the award of computer service contracts to private firms. Eckerd said he was not aware of any direct participation by NBS in providing for the security of specific agency procurements. Eckerd did say, though, that GSA and NBS were working together to produce "the necessary methods and procedures needed for adequately specifying security requirements in ADP procurements."

To the question, how can Government agencies be sure private companies maintain facilities and procedures sufficient to secure personal data and other sensitive information, Eckerd said:

> GSA cannot make assurances concerning specific efforts of other agencies and private firms. We can, however, assure the committee that GSA fully recognizes that Government has reached a point where something more than good intentions are needed; and that in regards to our responsibilities stemming from the Privacy Act of 1974 and OMB Circular A–108 we have appropriately amended procurement regulations and appropriately structured our teleprocessing service program. . . .

> GSA has no specific Governmentwide responsibilities for computer security, and as such we could be viewed as overstepping our authorities by seeking such assurances on the behalf of contractors or agencies. It is implicit in our regulations that the agency consider the security dimension of its requirements prior to using a commercial source. For those programs GSA is responsible for, such as the teleprocessing services program, it would be relatively easy to explicitly embrace considerations beyond the protection of personnel privacy, to include broader computer security issues. Such changes would also reflect the position that providing of computer security is the responsibility of the heads of agencies (not GSA's) and the fact that there are no Government-wide standards for computer security. On a case-by-case basis agencies must develop clear and definitive statements of security requirements and then judge the suitability of vendor offerings.

On the subject of personnel background checks regarding employees of contractor firms providing computer services to the Government, Administrator Eckerd had this to say:

> We have no reason to doubt that personnel reliability has a high priority among computer contractor firms as it does within the Federal Government. A prudent management will seek to insure satisfactory performance on any existing contract and to build a reputation which will invite future contracts. It is reasonable to expect, therefore, that such firms will seek out and eliminate cases of unreliable personnel. On the other hand, Federal agencies lack authority to require background investigations of employees of a contractor as a condition of a contract with two exceptions. Those exceptions are contracts in which defense classified information is involved and contracts made by GSA for guard and janitorial services in GSA-controlled buildings and storage facilities.
>
> It can be argued that because agencies have an obligation to husband and protect the Government assets, they are empowered to take those specific measures they deem necessary to discharge that general obligation. In this view, agencies already have sufficient authority to require background investigations of contractors' employees. On the other hand, the Privacy Act of 1974 places restrictions on the gathering and handling of personal information. It is reasonable to expect that lack of specific authority would engender challenge and delay when investigations of personnel were requested, thus impeding the procurement process.

GSA was asked to respond to the three reports on computer security and operations issued by the General Accounting Office in the spring of 1976.

The May 10 report, "Managers Need To Provide Better Protection For Federal Automatic Data Processing Facilities," had GSA's endorsement. Administrator Eckerd said GSA was fully supportive of

GAO's recommendations regarding the specific designation of security officials at Federal computer facilities and the use of FIPS-31 by agencies when developing and implementing physical security and risk management programs.

Eckerd said it is GSA's position that GSA or OMB should act on GAO's recommendations by (1) requiring the designation of a security officer for each Federal computer facility and take necessary actions to define the authority and responsibility of that position; and (2) requiring the review of security within each Federal computer facility and then assessing that review in light of a risk analysis of areas that needed to be improved.

Eckerd asserted, however, that he was not necessarily advocating that agencies establish a new and separate position of "security officer" at each computer facility, although, he added, that course may be necessary in some cases. Moreover, as another qualifying observation, Administrator Eckerd said FIPS-31 should not, at this time, be made mandatory but should remain—as NBS intended, he said—an "advisory guideline." Eckerd said FIPS-31 should not be made mandatory until sufficient experience with it, including cost considerations, had been realized.

Eckerd added that at the present time GSA and the Office of Management and Budget are working together to develop an effective approach for implementing Government-wide "guidance" in computer security.

Next, Eckerd commented on the GAO report, dated April 23, 1976, named, "Improvements Needed In Managing Automated Decisionmaking By Computers Throughout The Federal Government."

In response to that report, Eckerd said, OMB, on May 29, 1976, requested that GSA (1) review each GSA computer operation to determine whether any of them involved automated decisionmaking applications as defined in the GAO report; (2) review all administrative procedures, criteria, and computer programs pertaining to automated decisionmaking applications, to assess the possibility and probability of improper actions, the extent to which improper actions had or may be occurring and the monetary value of these improper actions; (3) identify and implement any improvements needed to minimize the future occurrence of improper actions; and (4) review and analyze existing policies, responsibilities, and procedures relative to the design, development, test, evaluation, and approval of automated processes and systems and to assure maximum efficient, effective, and economical utilization of these resources and develop any new policies, procedures, guidelines, or methodologies as necessary.

Accordingly, Eckerd said, GSA made a review of its computer operations and identified five systems which contained automated decisionmaking processes. Eckerd said GSA is continuing to review these systems to evaluate their accuracy. GSA will report its findings to OMB, Eckerd said.

Similarly, OMB, on June 16, 1976, instructed GSA to review the recommendations contained in GAO's report, "Computer-Related Crimes in Federal Programs," Eckerd said. That report, dated April 27, 1976, reflected OMB's concerns, Eckerd said, and GSA was directed to take appropriate actions as soon as possible to reduce the potential for computer-related crimes in ADP programs. Eckerd said

OMB requested that GSA consider implementing GAO's recommendations throughout the agency. Eckerd said a communication was sent to all GSA services and staff officers and to each GSA region requesting such a review with appropriate reply. Eckerd said that replies received indicated that GSA user systems are in compliance with GAO's recommendations.

Eckerd said GSA agrees with the GAO recommendations to set up (1) an organizational plan that segregates the duties of individuals to minimize their opportunity for misuse or misappropriation of the computer system's resources; (2) a system of authorization and record procedures sufficient to provide effective accounting control over assets, liabilities, revenues, and expenses; (3) an established system of practices to be followed for each duty and function of the organizational unit involved in the computer system; and (4) an effective system of internal review, including an internal audit staff that has training adequate to review and evaluate computer-based system controls and that does such reviews both when systems are being designed and after they have become operational.

"GSA agrees with the recommendations made by GAO and will continue to make every effort to apply the principles to both our manual and automated systems," Eckerd concluded.

AN EVALUATION OF INFONET SECURITY

Time sharing, in computer terminology, means the utilization of computer or data banks by many individuals, or users, from remote terminal devices at the same time.

A major time-sharing capability used by Federal agencies is a computer system known as Infonet. Infonet is owned by a private firm known as Computer Sciences Corp. Infonet offices—that is, the Information Network Division of the Computer Sciences Corp.—are at 650 North Sepulveda Boulevard, El Segundo, Calif. In this section of the committee's staff study Computer Sciences Corp. will be referred to as CSC.

Some 200 Federal departments, agencies, and offices use Infonet's commercial time-share system. Government use of the Infonet time-share system is a result of contract GS-00S-11580 entered into by the General Services Administration's Automated Data and Telecommunications Service (ADTS) with CSC. Besides the approximately 200 Federal users of Infonet, Infonet also has subscribers from the private sector.

According to report No. 20-5002-CAC of the Office of Audits, GSA, dated February 18, 1976, Infonet's hardware consists of a number of Univac model 1108 computers with associated computers, disk, and drum storage devices and communications equipment in El Segundo, Calif., and Oak Brook, Ill., and a connecting communication system.

The GSA Office of Audits report said CSC permits the Government to access the Infonet network through communications ports in Boston, New York, Washington, Atlanta, Huntsville, Chicago, St. Louis, Fort Worth, Dallas, Denver, San Francisco, Los Angeles, Auburn, and Seattle. In computer terminology, access can be defined as the ability and the means necessary to approach, to store or retrieve data, to communicate with or to make use of any resource of an automatic data processing (ADP) system.

The GSA Office of Audits report said that in terms of software Infonet provides basic FORTRAN, COBOL, and assembler programing languages, a proprietary data management language, management information systems, general purpose utility programs, and an application library.

GSA said that originally the contract with CSC—No. GS-00S-11580—ran through June 30, 1973, with options for three annual renewals. GSA exercised two options to renew the contract through June 30, 1975. CSC and GSA agreed to extend the contract through June 30, 1976. The new agreement, GSA said, also provides that if CSC is awarded a contract under the multiple award schedule contract teleprocessing program, all Infonet users except the GSA Federal Buildings Fund will transfer to the new contract.

GSA's contract with Computer Sciences Corp. (CSC) makes Infonet the largest single commercial computer time-share system under contract to the Federal Government.

According to GSA Administrator Jack Eckerd, billings by Infonet to Federal user agencies in fiscal year 1974 were $11,279,495. In fiscal year 1975, these billings totalled $19,409,308. For fiscal year 1976, the billings came to $25,718,866. The Federal user agencies included GSA, the Army, Navy, HEW, Agriculture, HUD, Postal Service, Defense Contract Audit Agency, Energy Research and Development Administration, General Accounting Office, Department of Defense, Small Business Administration, Interior Department, Federal Energy Administration, Commerce, NASA, Treasury, Federal Trade Commission, Civil Service Commission, Office of Management and Budget, and other agencies.

Owing to the considerable amounts of information the Federal Government stores and processes in the Infonet system, officials were concerned about the adequacies of Infonet's security precautions. Accordingly, in the fall of 1974, GSA entered into contract No. GS-035-43811 with the Stanford Research Institute (SRI), Menlo Park, Calif. Under the terms of this contract, SRI was to assess the security of the Infonet system and of its use by Government users.

The SRI team was headed by Donn B. Parker, a senior information processing analyst at SRI. Parker, who has performed computer security research for the National Science Foundation and the General Accounting Office and, as an author and lecturer, is quite well known in the ADP community, was assisted in his Infonet security evaluation by D. N. Berg, D. H. Brandin, H. L. Holden, N. R. Nielsen, W. D. Tiffany, and P. M. Whiting-O'Keefe. Parker's report, completed January 31, 1975, and revised April 1, 1975, is named "Security Assessment of the Infonet System and Its Use By the Federal Government."

GSA Administrator Jack Eckerd, in his November 9, 1976 statement submitted to the Senate Government Operations Committee, referred to Parker's SRI study. Administrator Eckerd said that Parker's team had concluded that Infonet's security features were "commensurate with the uses being made of the system." Eckerd did add, however, that the SRI report indicated there did exist "opportunities to further enhance the data security of Infonet." Eckerd also acknowledged that any shortcomings in the security apparatus at Infonet were not the fault of the Infonet security safeguards but were, instead, the result of inappropriate or incomplete actions taken by users, users in this case being Federal agencies.

It was the view of the staff of the Senate Government Operations Committee that an evaluation of the security precautions in the Infonet system could not be an accurate evaluation, from the Government's point of view, unless it took into account both user and contractor practices, procedures, and habits of transacting ADP communications. In that light then—that is, when the Federal use of Infonet and Infonet are evaluated as a whole—Parker's SRI report on Infonet security procedures takes on a meaning different from the meaning as characterized by GSA Administrator Eckerd. The title of the SRI report, "Security Assessment of the Infonet System and Its Use By the Federal Government," reveals that it was the Parker team's intention to evaluate not only Infonet's security procedures but to also examine the security procedures of Federal users of the Infonet system.

Moreover, it was in their evaluation of the security practices of the Federal agencies using Infonet that the SRI investigators found fault. The Parker report, as GSA Administrator Eckerd said, exonerates Infonet itself, for the most part, of serious security failures. But the users—that is, Federal agencies—fared less well in the SRI study. As the study asserted, "The overall security provided by Infonet meets and in some ways exceeds the low level of user demands and is consistent in many ways with current practice to the extent that has been determined through SRI experience." But the Parker team went on to say, "At present the greatest risks to the general level of security of Government data on Infonet are the users' lack of security awareness and failure to use available security precautions." The Parker team added, "By far the larger source of general security risks are the users. The security risks associated with the system, while clearly present, are of lesser concern and import."

The SRI report found, for example, that data stored on the Infonet system by Government users ranged from nonsensitive to very sensitive and the knowledge and sophistication of the user community ranged from "naive to expert." The Parker team investigators said they came upon instances in which Government users of Infonet did not fully comprehend the sensitivity of the data in their files and the need for appropriate higher security measures. No general guidelines were observed covering the sensitivity of information and the proper handling of such information, the Parker group said.

The SRI team concluded improvements were needed in the manner in which Government users of Infonet managed passwords. In computer terminology, a password is a protected word or a string of characters that identifies or authenticates a user, a specific resource, or an access type. Password is synonymous with keyword.

The Parker team pointed out that anyone obtaining someone else's password can make himself appear to the computer system as if he were the legitimate holder of the appropriate credentials to gain access to data. Parker's investigators discerned a "lack of proper treatment of passwords" by Federal agencies linked to Infonet.

The SRI report demonstrated the password problem by citing instances in which passwords were printed on terminal output paper, thereby exposing the password to unauthorized personnel who might be passing by. In other illustrations drawn by the Parker team it was noted that documents carrying passwords were left unattended lying on tables and counters in terminal areas.

In addition, the Parker team said, passwords were frequently selected for the convenience of the user rather than to strengthen security. Passwords were selected for ease of recall, Parker said, citing instances in which passwords were formed from a user's initials, family name, address or project title. In other cases, the Parker team said, passwords were not changed frequently enough, thereby increasing the possibility that an unauthorized person might learn it.

Parker went on to say:

> Users sometimes incorporate passwords into programs for a variety of convenient reasons. However, when these programs are subsequently stored in shared files, detection of the password is readily achieved by others accessing that shared file. By exploiting such user oversights during terminal sessions on Infonet, SRI obtained several user identification numbers and passwords. This placed SRI in a position where it could have copied, changed or destroyed any of the data files associated with those users' accounts. The skills and knowledge of the SRI user who was able to accomplish this are comparable to any experienced application programer who has had previous timesharing computer usage experience. Such users have gained a general knowledge of how computer systems may be organized. Such users generally have knowledge of several programing languages and experience in processing data from large disk and magnetic tape files.

The SRI report next addressed itself to "access control," saying that, for the most part, little control was maintained over access to terminals and to terminal output at user locations. Thus, the Parker team noted, sensitive information could, in many instances, be compromised in the terminal area while located entirely outside the computer system.

As for capabilities provided by Infonet itself to secure the computer system for Government users, the Parker team concluded Infonet was doing a good job. Some of these security features were inherent in the design of the Infonet system, the SRI report said, while other security features were available as user options. These optional features had to do with access limitations, selective authorizing procedures and additional password safeguards. "However," the Parker team said, "many users are unaware of the optional capabilities and, therefore, do not take advantage of them." Similarly, SRI's investigators said, some Government agency users of Infonet knew about the optional security procedures but decided not to use them—or, if they did use them, did not utilize them in a safe or appropriate manner.

The Parker team called attention to an Infonet service allowing for Federal users of the system to keep track of computer use. This "log information" can monitor system usage so that accounting errors and unauthorized account access can be detected. Once again, however, the Parker team said, some Government users, particularly users other than GSA, were not currently receiving this information.

The Stanford Research Institute group noted that Infonet had built a comprehensive security system for its operation. But, the team said, little attempt had been made to monitor protective mechanisms. The Parker group said, for example, that there was a protective mechanism within the computer system to make it difficult for persons to make repeated attempts to guess an account's password. The Parker team said Infonet disconnected a user after three failures to specify the correct password but did not monitor the number of invalid attempts. Therefore, the Parker team said, one user can repeatedly attempt to read another user's protected files and no alarms or other signals would be initiated indicating that such attempts had been made.

The SRI report said that there were 30 to 60 Infonet employees who had the capability to access user data files. The report said there was no monitoring to determine if accesses were made to user accounts by Infonet personnel. The Parker group also noted that there was no internal audit capability within the Infonet operation.

The Parker team said Computer Sciences Corp. (CSC) had developed a comprehensive set of documented policies and procedures relative to security at its El Segundo facility. "Impressive" was the term the Parker team used to describe CSC's concern for security, as judged by the security policies and procedures. But, while the policies and procedures existed on paper, they were not always enforced, the Parker team said, pointing out, for example, that CSC did not enforce its own password selection procedure. Because the password procedure was not in place, the Parker team said, SRI investigators, assuming the role of ordinary users, were able to gain access to an Infonet account carrying privileges not extended to other users. In another instance, the Parker team said, the GSA Office of Audit recommended that two of the alarmed building doors be tested. They were tested and the alarms did not sound, the SRI report said.

The report said that CSC assigned the responsibility for the security of Infonet to one person. That person had many other responsibilities which took time away from his Infonet security responsibilities. The Parker group said there was no person whose primary responsibility was computer security. Moreover, the SRI report said, there was no periodic operational audit and reporting that included examination of the Infonet system by internal or external auditors. The Parker group said that because of this lack of audits there was no way that CSC management could routinely be informed of the overall state of Infonet security except for possibly holding reviews conducted by Infonet management responsible for security.

SRI examined the safeguards against entry by unauthorized persons into the Infonet computer rooms. Entry to the computer rooms was controlled by two levels of perimeter protection and a badging system. Access to the building in which the computers were located was controlled by a guard or receptionist and alarm-controlled doors. But the Parker group concluded this protection was not totally effective. The Parker report said CSC itself reported the presence of unauthorized persons in the Infonet operations building but not in the computer rooms or other specially restricted areas. SRI said no special fire detection facilities were provided in most computer areas and that fire protection was limited to hand held fire extinguishers.

Users' magnetic tapes were stored on open racks in the computer rooms close to the computing equipment, the Parker team said. In addition to exposure to the normal hazards of the computer room, the tapes were accessible to all computer operations staff, the Parker group said, going on to say that no backup copies of user tapes were routinely stored remotely and that users had never been explicitly told about tape handling and storage procedures. Parker said users had not been informed of the need for additional safety for storage and backup of sensitive or critical data on tape. But, the SRI report said, CSC had indicated it would provide such services upon request.

Just as magnetic tapes were stored in the computer room, the Parker group said, backup copies of disk files were also stored in the computer room. But data was removed to a storage vault on a weekly basis. The storage vault adjoined the CSC building in El Segundo but the vault was not an integral part of the facility. The Parker group said the vault provided some disaster protection but it could not be considered far enough away to be an offsite location. Accordingly, the Parker team said, security of the backup copies of disk files was not sufficient in the event of disasters such as fire, explosion, or earthquake. Computer Sciences Corp. did send some data to its Oakdale, Ill., facility for added protection, the SRI report said. In turn, the report said, an offsite vault outside the immediate vicinity of the CSC facilities in El Segundo did not exist. Such an offsite vault would have to be close enough for physical access to restore service within a reasonable time, the SRI report said.

The SRI report explained that magnetic tapes that are not produced on the Infonet system, or magnetic tapes that are destined for other systems, are termed "foreign tapes." The Parker team said that from a security viewpoint operational procedures used for foreign tapes were weak. In particular, Parker's SRI report said, the external labeling procedures for foreign tapes were inappropriate. As a result, Parker said, the data on foreign tapes was subject to accidental and deliberate compromise. However, the report noted, CSC indicated it would improve the labeling procedures, bringing them up to a more appropriate level of security.

Next, the SRI report addressed itself to the subject of telecommunications. Terminals communicated with the central computers through commercial telephone systems, the Federal Telephone System (FTS) and Infonet's Remote Communications Concentrators (RCC) located in Infonet offices in major areas of user concentration.

The SRI report said:

> The RCC is a programable (computer) device providing multiplexing and error control and allows use of a variety of terminal types and operation speeds. The RCC sites are under access control similar to that provided at the computer facility. The RCC's are manned part time by operators. The remainder of the time they run unattended. No special precautions are taken in the placement of circuit boxes or telephone lines within or leading from buildings. The telephone lines at the El Segundo facility are underground. There is no special redundancy of circuits other than normally provided by the telephone

> companies. An area of unknown level of security for telecommunications is within the jurisdiction of the commercial telephone companies but is outside the scope of this study.

The Parker team then went to the subject of "service continuity and disaster protection." On this issue, the team said the unavailability of service at crucial times or for long periods of time can be a serious security concern. As an example, the Parker group said, a Government agency could suffer a significant loss if a user is denied access to information or processing in a time-critical transaction. In addition, the report said, the extraordinary conditions caused by a system or operational failure could seriously weaken or compromise normal security functions.

SRI said that, while safeguards to protect building security did exist regarding nonforcible and nonviolent entry, a variety of ways were available by which the CSC headquarters facility containing the Infonet El Segundo operation could be entered by hostile persons. There were also a number of ways in which the operation of the computer systems could be halted by internal or from external hostile persons, the Parker group said. Parker added that forcible assaults were rare but they had occurred.

The Parker team said there was no backup or uninterruptible power supply for the El Segundo operation. But, the team said, there were two Southern California Edison power sources, to be switchable in the future, entering the building. There were no definite plans for shifting the El Segundo processing load to the Oakbrook, Ill., system should service be interrupted by disaster, the SRI team said. The Parker group said that GSA had not provided Infonet the requested Government service priorities and account priorities for special treatment in such an event.

The Parker team said the GSA-Infonet contract specified service continuity requirements and provided for liquidated damages in the event that these requirements were not met. The Parker group said that this removed to a degree the disaster recovery considerations from the concerns of the Government user.

The SRI report explained:

> How CSC chooses to meet its contractual obligations is legitimately its own business decision. However, data of considerable value (e.g., instructions for Treasury disbursements) are stored in Infonet. Although SRI cannot estimate the potential damages that could result from the unavailability of this data, no evidence was found that users had made such a determination and related their potential damages to the contractual damage clauses.

The Parker group, still discussing Infonet's "service continuity and disaster protection" capabilities, said the fire detection and extinguishing equipment located in the computer areas was not adequate "even though CSC claims it meets local fire code requirements." The SRI report said equipment provided the Oakbrook facility was more appropriate for a large-scale, on-line, multicomputer system.

The Parker group said Infonet had assembled a capable staff to assist users with specific problems occurring in their use of Infonet services. In addition, a number of manuals had been published covering major aspects of the system and its services, SRI said. But in this literature and services, SRI said, there were two considerations affecting security.

The Parker team explained:

> One area concerns the provision of information that is not needed by the user. Thus, certain account number data (excluding passwords) are needlessly available in public files. Diagnostic messages on security violations are, in some cases, overly explicit, thus providing helpful information to the potential penetrator.
>
> The other area concerns the provision of information about the use of security-oriented characteristics of the system. Very little consolidated information is now provided to the user with respect to his ability to enhance the security of his Infonet usage. He generally lacks a central source of specific information about the security features available, the use of these features, and the security side effects and pitfalls associated with the Infonet system.

On July 28, 1976, Donn B. Parker told the Committee that the audit of Infonet was limited as a result of an agreement with officials of the Computer Sciences Corp. Parker said he refused in his report to assert that security was adequate at Infonet because of a lack of standards to measure Infonet's security system against. He said that in testing the Infonet system he "did not go all the way in attempting to get into any other customer's files." Parker said he did not initiate an exhaustive effort to crack the Infonet system. He said an expert in penetrating computer systems could have compromised Infonet with a concerted attack on the system. Parker also said that during the audit he did not have access to the Infonet operating system.

THE PHILIP A. TENKHOFF STATEMENT

Philip A. Tenkhoff was the director of systems development for the Information Network Division (Infonet) of Computer Sciences Corp. Tenkhoff had responsibility for the planning, network design, specification, and implementation of all hardware and communications for Infonet. Tenkhoff was also responsible for directing the long-term evolution of the Infonet network and was responsible for the overall security of the network.

On August 2, 1976, Tenkhoff sent to Government Operations Committee staff a copy of a speech he, Tenkhoff, was to give that week to the International Conference on Computer Communication. The Conference was held in Toronto. In his letter to the staff, Tenkhoff said he was providing the text of the speech to indicate "some general information concerning Infonet's approach to security." Because Infonet is the largest commercial computer time-sharing contractor with the Federal Government, because information provided the committee by the General Services Administration (GSA) revealed that Infonet will, in all probability, continue to increase in the services it provides Government and because the Stanford Research Institute

(SRI) evaluation of Infonet detected shortcomings in the Infonet-Government user security procedures, this staff study will now report on Tenkhoff's speech regarding his organization's approach to security.

Tenkhoff said data security had long been an essential consideration for remote teleprocessing systems. Tenkhoff said a stringent level of security must be provided to protect the interests of multiple subscribers using a shared system. He said that for many major networks, design considerations which reflected the concern over data security preceded increased legislative attention toward data privacy. While his remarks in this speech related specifically to Infonet, Tenkhoff said, much of what he had to say could be applied to the remote computing industry as a whole.

Tenkhoff said each subscriber to Infonet had one or more terminals located in one or more cities throughout the United States, Canada, or Europe. Each terminal accessed the centralized host computers through special communications concentrators which are located in Infonet facilities, he said, adding that access was achieved through both the public switched telephone network and dedicated circuits. In computer terminology, a dedicated mode is defined as the operation of an ADP system in which the central computer facility, the connected peripheral devices, the communications facilities and all remote terminals are used and controlled exclusively by specific users or groups of users for the processing of particular types and categories of information.

Tenkhoff said the Infonet communications network used dedicated common carrier circuits and routed all communication to the centralized host computers. He said that subscriber data files and programs were stored on magnetic disks or tapes located in the computer center.

Tenkhoff said increased legislative attention had recently been directed toward privacy and security in data processing systems. These legislative actions, he said, had brought into the open the interrelationships and conflicts regarding individual rights to privacy, the current state of computer technology, and the cost of providing computer security. Computer designers and services suppliers are faced with the challenge of providing systems which meet the security objectives of a wide range of user requirements for privacy and security in a competitive economic environment, Tenkhoff said.

Referring to the Stanford Research Institute evaluation of Infonet, Tenkhoff said that because of Infonet's unique role as a supplier of remote data processing services to the Federal Government Infonet had been subjected to the first government audit of such a service in terms of security.

Tenkhoff said important factors in a commercial firm's ability to provide ADP services to the Government are privacy, security, and reliability—but that all too often these three considerations are all linked together rather than being viewed individually.

Privacy, Tenkhoff said, is a legal issue and not a technical one. He said that for a computer network, such as Infonet, privacy deals with actions associated with the content and disposition of data files which are created by various commercial and Government agency subscribers. The content of these files is determined solely by the user, Tenkhoff said, explaining, "Thus, the responsibility for their content must rest totally with that user. Only he should be held accountable for any legal violations."

On the subject of security, Tenkhoff said computer security related to the technical means by which the integrity of the user's data is preserved. This, he said, included protection against alteration, loss, or disclosure of a user's data. Tenkhoff said security included a total range of means including hardware design, physical protection, operations, and personnel procedures. The supplier of network services must provide the required security and the subscriber must appropriately use the security features of the system, Tenkhoff said. "Hence, security must be viewed as a joint supplier and user responsibility," Tenkhoff said.

This last observation by Tenkhoff—that is, that computer security is a joint responsibility of both supplier and user—supported the Senate Government Operations Committee staff's view, articulated in the previous section of this staff study, that to say Infonet's security procedures are sound is merely to attest to the capability of one-half the equation. The other half of the equation must be that the users of Infonet—that is, Federal agencies—effectively utilize those security procedures.

Next, Tenkhoff discussed reliability of the Infonet system. He said reliability was associated with the degree to which user files were available upon demand from a subscriber. This, he said, included consideration of both downtime—that is, when a computer is not available for use—due to temporary interruptions and the protection against irrevocable loss of files, including natural or civil catastrophe. Reliability, Tenkhoff said, is the prime concern of the services supplier.

On the subject of system architecture, Tenkhoff said the system software design for Infonet had, as one of its principal objectives, the assurance of providing a high level of security. The majority of this design, he said, was accomplished in the 1969–71 time period. Infonet's motivation was to protect the unauthorized disclosure of a client's data to any other source, be the disclosure through accident or intentional system penetration.

Tenkhoff said the system architecture of Infonet provided four principal categories of protection: (1) entry protection; (2) file protection; (3) sharing protection; and (4) penetration protection.

Entry protection, he said, dealt with the controls imposed by the system over both access to the Infonet system and to specific files within the system. Each subscriber has a user identification number and a password, Tenkhoff said, adding that the essential key which provides access to the system is the password. The password, he said, consists of six characters, any one or all of which could be randomly selected by the user from a set of more than 100 alphanumeric and control characters leading to a potential of 10^{12} randomly selected 6-character passwords.

Tenkhoff said Infonet provided the user the capability to change the password at any time. Such a change would be done by the user from a terminal without intervention by Infonet personnel, Tenkhoff said. He explained that customers are encouraged to change the password frequently and to choose their password in a random fashion.

Tenkhoff went on to say that a higher level of access protection was provided as an option. This capability, known as autolog, permits a customer to design and impose additional security precautions. For example, he said, a user could design multiple passwords to gain access to data. For added security, Tenkhoff said, a customer could have the system automatically change the password and simultaneously create a complete audit trail of attempts to enter the system. In computer terminology, an audit trail is defined as a chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

Tenkhoff said that once the proper user identification and password are provided and the user is authenticated, there is an additional level of security at Infonet known as file protection. He said file protection included the ability of the user to assign special attributes to individual files under his control. Tenkhoff said that examples of file protection in the Infonet system were "execute only" and "limited access." Tenkhoff said "execute only" means that access to files can be executed only by designated users. Files cannot be read, changed or deleted. He said that "limited access" files may only be accessed by a special program and that general access is prevented.

Tenkhoff said that users with requirements for even greater levels of file protection may encrypt their data. In computer terminology, encrypt means to convert plain text into unintelligible form by means of a cryptographic system. Tenkhoff said Infonet enables the user to write encryption routines which store all or part of his data in an encrypted fashion. With this approach, he said, the scheme selected by the customer remains known only to that customer and is not available either to other customers or Infonet employees. In addition, Tenkhoff said, Infonet provided a standardized encryption routine available to all users. With this approach, he said, the user provides the encryption key which provides an assurance that unauthorized users cannot break the encryption algorithm. In mathematics, an algorithm is any mechanical or recursive computational procedure.

Tenkhoff said that the third form of system protection—after entry and file protection—was sharing protection. He said the Infonet system was structured around individual libraries. He said a capability is provided to permit libraries to be shared among users. Sharing of certain specified system libraries is automatic, Tenkhoff said, explaining that sharing between user libraries was at the sole option of the affected users.

Infonet provides users with three different levels of sharing, Tenkhoff said. The decision as to which level to choose from is up to the user, he said, depending on the user's security requirements. Tenkhoff said the first level is "unrestricted" sharing in which the sharer of the library has the same privileges as the owner of the library. The second level is "restricted write" in which the sharer may read any level in the share library but may alter or delete only those files which he has contributed. The third level, Tenkhoff said, was "restricted read" sharing in which the sharer may read files in the library but may not alter, delete or contribute to the library.

Tenkhoff went on to discuss "intraaccount" sharing. He said intraaccount sharing was accomplished under the direction of the customer account manager. Intraaccount sharing is achieved by Infonet, he said, only after written consent was received from appropriate management of the affected accounts. Tenkhoff said it was noteworthy that the architecture of the Infonet system was such that sharers need not know each other's user identification or passwords.

The fourth protective procedure, Tenkhoff said, is known as "penetration protection." This form of protection includes those architectural features of the system which secure the system against accidental or deliberate penetration. For example, Tenkhoff said, Infonet and UNIVAC jointly developed a full memory protection at the hardware level for all user and system programs. This facility provides a hardware interrupt of the operating system if any user program attempts (1) to access any memory area outside of those predefined for his exclusive use; (2) to perform any instruction that would violate the security envelope; or (3) to make any changes in the instruction area of the user program, Tenkhoff said. He explained that this memory protection feature is provided automatically to all users and that no specific customer action is required. Tenkhoff said other types of proprietary protection are also provided at Infonet but that disclosure of these features would be a violation of proprietary and security considerations.

Physical security at Infonet was then described by Tenkhoff. He said extensive precautions had been taken to maintain the integrity of the physical facility in which the Infonet computers were located. He said the centers are located in buildings to which 24-hour access control is rigidly enforced. He said specific coded badges are required for entrance to the computer areas. He said these badges are issued only to persons directly involved with the operation and maintenance of the computers and communications network. Visitors and other employees were prohibited entry, he said.

Tenkhoff said continuous surveillance and monitoring by uniformed guards were employed to enforce building access regulations. In addition, he said, access to the computer areas was rigidly controlled by locked doors, each of which contained cipher locks whose combinations were changed at specified intervals.

Tenkhoff, addressing himself to operating procedures, said an integral part of a complete computer security system required establishing and maintaining proper operating procedures. He said Infonet maintained a complete set of "operations policies and procedures." These contain the requisite security measures which must be followed in the operation of the system, Tenkhoff said.

He said that Infonet decided to incorporate security procedures directly into the overall operating procedures in lieu of issuing a separate operations security document. It was felt that this approach would provide a continuous reminder of the security-related aspects of all operations functions for the personnel involved, Tenkhoff said.

Tenkhoff said some examples of procedures that contain security-related functions included those associated with the accounting and control of user programs and output, appropriate handling of inquiries regarding use of the system physical access control and emergency procedures.

A principal focus of this staff study has to do with personnel security and the procedures followed by the executive branch in clearing workers in Federal computer programs and in Federal contractor computer programs. It was a preliminary finding of the Senate Government Operations Committee staff that procedures aimed at attesting to the suitability of employees in computer programs was not consistent, both in Government programs as well as programs contracted out by agencies to commercial firms. Tenkhoff, speaking for the largest single Government contractor time-share firm, Computer Sciences Corporation's Infonet, said his organization was cognizant of the sensitivity of personnel hiring and evaluation practices. However, in his speech before the International Conference on Computer Communication in Toronto in August of 1976, he gave no specifics as to how Infonet cleared its personnel. He said that any security system was dependent to a large extent on the personnel who operate and maintain the system. In addition to providing a secure architecture and proper procedures, he said, continuous attention must be paid to personnel selection and training. Employee awareness of the critical nature of security to the entire business of remote computing must be continuous, Tenkhoff said. He said that periodic reviews were held by Computer Sciences Corporation to insure that personnel were being appropriately attentive to security procedures. Tenkhoff made no reference to the manner of background checks Infonet conducts concerning persons employed or applying for employment.

Tenkhoff discussed the trade off which Infonet management has to make concerning security precautions and their cost. Independent inquiry by the Senate Government Operations Committee staff indicated that most experts in the computer field were of the opinion that it was virtually impossible to secure a computer system against every conceivable compromise or form of physical damage. As Tenkhoff put it, "There is a direct relationship between increasing levels of security and increasing cost." He added, "This is a fundamental dilemma for the supplier of computer services in a shared environment." Tenkhoff said Infonet had chosen to solve this dilemma by providing a high level of security for all users with optional levels of additional security for those users with extremely critical data requirements. In this way, he said, the user with modest security needs does not have to pay the price, in both cost and inconvenience, for extremely high security requirements. He said that experience had shown that the standard level of security provided on Infonet was appropriate for about 99 percent of all applications. He said the remainder of the clients invoked the optional features to obtain additional levels of security.

Tenkhoff, making his own reference to a point made by the Stanford Research Institute team under Donn B. Parker, said that a major problem which had been repeatedly observed was that many users did not take advantage of the security features which Infonet makes available. This assertion by Tenkhoff was similar to an observation made by Parker's SRI group in which it was stated:

> At present the greatest risks to the general level of security of Government data on Infonet are the users' lack of security awareness and failure to use available security precautions.

The Parker group also noted:

> In the course of its examination SRI has uncovered what are believed to be shortcomings in the security associated with the Government's use of Infonet services relative to the sensitivity of the data it stores in Infonet. Many of these weaknesses are the result of user action—and inactions—and as such are not the responsibility of Infonet. Other weaknesses are the responsibility of Infonet. However, some of these latter findings can be viewed more as a criticism of the user community and the industry than of Infonet.

Tenkhoff said Infonet had tried to determine why its clients had not invoked those security safeguards available to them. He said three principal reasons were found. First, he said, many users were unaware of their responsibilities to insure the security of their data files. Tenkhoff said users tended to use the computer system without explicitly considering their particular security requirements. For example, he said, a subscriber who selected a password which was identical or similar to his company's name was not fulfilling his responsibility for security. Tenkhoff stressed, ". . . the password is the key to the system. Each subscriber must protect his password in a rigorous manner. Passwords should be changed frequently; their dissemination within a company must be methodically controlled and different user groups within a major subscribing company should have independent password systems."

Similarly, one of the Stanford Research Institute's strongest criticisms of Federal use of Infonet had to do with lax procedures concerning passwords. The Parker team said anyone obtaining someone else's password could make himself appear to the computer as if he were that person, thereby gaining access to the person's files. "Although most users were aware of the need for passwords," Parker said, "there is frequently a lack of proper treatment of passwords."

The SRI group went on to say:

> . . . in some cases passwords are needlessly printed on terminal output paper. This fosters compromise from passers-by. In some facilities card decks containing passwords are frequently left lying on tables and counters at batch input/output terminal locations. Passwords are frequently selected for the convenience of the user rather than to maximize security. A typical instance of this is the password picked for ease of recall and related to the user's initials, family, address or project name. In some cases, passwords are not changed frequently enough to reduce the possibility of compromise.
>
> Users sometimes incorporate passwords into programs for a variety of convenient reasons. However, when these programs are subsequently stored in shared files, detection of the password is readily achieved by others accessing that shared file. By exploiting such user oversights during terminal sessions on Infonet, SRI obtained several user identification numbers and passwords. This placed SRI in a position where it could have copied, changed, or

> destroyed any of the data files associated with those users' accounts. The skills and knowledge of the SRI user who was able to accomplish this are comparable to any experienced application programer who has had previous time-sharing computer service usage experience. Such users have gained a general knowledge of how computer systems may be organized. Such users generally have knowledge of several programing languages and experience in processing data from large disks and magnetic tape files.

To counter password laxity among Infonet users, Philip A. Tenkhoff said, Infonet had recently produced a user-oriented document entitled, "An Introduction to Infonet Security." The purpose of this document, he said, was to provide users with information about Infonet security so that they would be aware of the security features of the Infonet system and so that they could design their applications according to particular security needs.

Besides their lack of consideration of their own security needs—as exemplified in password laxity—Infonet users were making a second mistake, Tenkhoff said. This second of the three user shortcomings, Tenkhoff said, could be seen in the fact that users were careless and unattentive to proper security procedures. In this regard, Tenkhoff cited this example. He said some users had selected a random password and then posted that password in a conspicuous place and that unauthorized personnel could see it. This, too, compromised security, Tenkhoff said. And this user shortcoming was also one cited by the Stanford Research Institute team, as noted earlier in this Senate Government Operations Committee's staff study.

Tenkhoff said:

> Situations have actually been observed wherein users have taped their password to the terminal. One might compare this to keeping the safe deposit box key taped to the box so it is never lost.

The third cause of inadequate security, Tenkhoff said, had to do with convenience. Increased security, he said, carries with it the corollary of increased inconvenience. Some Infonet users, he said, were simply unwilling to accept this increased inconvenience. "Remembering a password of six randomly selected characters is more difficult than remembering a password which is associated with one's birthday," Tenkhoff said, adding, "Changing a password daily is less convenient than never changing it." Tenkhoff said that implementing, through Infonet's autolog procedure, a scheme which would require two people, each with his own password, to be present before a given file could be accessed is more difficult—and more inconvenient—than using a standard sequence for entering the system. Tenkhoff said many similar convenience versus inconvenience examples could be demonstrated.

Tenkhoff then said:

> Experience to date has firmly convinced CSC that the weakest link in the security of user data on shared remote computing systems is the user himself. Additional user oriented security education needs to be provided . . .

> When the using community as a whole begins to use all of the security safeguards which are available, overall data security will be considerably enhanced.

In his speech in Toronto, Philip A. Tenkhoff, director of System Development Organization, Computer Sciences Corp., then went on to discuss the examination of Infonet made by the Stanford Research Institute. He said it was the first such Government audit of a commercial shared remote computing service for computer security.

Tenkhoff provided background on how the SRI audit came about. He said that in 1972 Infonet was awarded a contract by the General Services Administration (GSA) to provide services to all Government agencies which required common data base, full service remote teleprocessing services. For users falling within the scope of the contract, he said, Infonet was a mandatory source of supply for the period June 1972 to June 1976. Under that contract, Tenkhoff said, there were no provisions for security audits. Infonet was, however, obligated to provide the degree of security called for in the Government's contract award procedures.

In turn, Tenkhoff said, with the increased Federal attention directed toward the areas of computer privacy and security, GSA requested that Computer Sciences Corp. allow an audit of Infonet. Tenkhoff said CSC was not required to submit Infonet to this audit but it permitted the audit "in the best interest of the Government."

SRI was selected by GSA's Office of Audit to conduct the study, Tenkhoff said. But, he explained, since there were no agreed upon "security standards," establishing a basis for the audit required close cooperation among GSA, SRI and CSC. Such issues as the protection of CSC proprietary data, protection of user data, dissemination of findings and audit methodology all required resolution before the SRI survey could begin, Tenkhoff said.

Under the terms of the audit agreement, Tenkhoff said, personnel from the GSA Office of Audit and SRI were permitted to have access to the computer areas, all operations procedures and operations personnel. A normal customer user identification and password were provided in order that system security could be assessed by the SRI team, Tenkhoff said. He said the audit and related analysis of findings was conducted over a period of 6 weeks.

The report issued by the SRI team described its ground rules in conducting the audit this way. The report said the security survey was restricted to a study of the Government users of Infonet, an examination of the Infonet service as it was "perceived at the user interface" and an examination of Infonet operations in El Segundo, Calif. The SRI report said that the GSA Office of Audits conducted its own examination of the Infonet operations in Oakbrook, Ill.

The SRI group, headed by Donn B. Parker, said its examination of Infonet was based on documents normally available to Government users, interviews with Government users, observations of Infonet service made from an SRI-supplied password and account number, interviews with Infonet personnel and observations made at CSC facilities in El Segundo.

The SRI investigators said the user interviews were conducted with a GSA-selected "pseudo-random sample of Government Infonet users." The sample included personnel from GSA and other Government agencies, the SRI report said. Users representing 14 of 234 permanent account numbers were selected for interviews, the Parker team reported. Those selected were primarily main users, the SRI report said. These main users accounted for about 50 percent of the total monthly storage charges for Government users of Infonet in June 1974. Parker said the sample was believed to be adequate, although the SRI team did acknowledge in its report that there are risks inherent in generalizing from such a sample group.

Tenkhoff said that Computer Sciences Corp. agreed, "as evidence of its concern for security," to amend its contract with GSA to provide for future periodic audits.

The staff of the Senate Government Operations Committee did not attempt to evaluate the accuracy of the SRI report. Nor did the staff seek to evaluate the accuracy of Philip Tenkhoff's assessment of the SRI audit. However, the following language from the SRI report may be useful in achieving a view of both the SRI report and Tenkhoff's comments about it. This language from the SRI report said:

> By prior agreements between GSA, SRI, and CSC, the security assessment placed reliance on materials and documentation voluntarily supplied by CSC, on statements which CSC personnel made, and on observations which CSC voluntarily permitted. Thus, the SRI study is a comprehensive but not totally independent analysis of Infonet system security. However, the excellent cooperation received from CSC personnel assigned to work with SRI did permit some independent verification of CSC-supplied information. In large measure, such independent verification supported the information supplied by CSC, although certain discrepancies (both favorable and unfavorable) were observed and reported in the findings section of this report.

Concluding his remarks in Toronto, Infonet's Philip A. Tenkhoff discussed the Privacy Act of 1974 (Public Law 93–579) and how Computer Sciences Corp. was seeking to comply with the law. Tenkhoff said that because of the large number of Federal agencies which use Infonet for their data base services, Infonet had a particularly strong interest in the Privacy Act of 1974, which became effective in September 1975.

Tenkhoff said the Privacy Act dealt with actions that must be taken regarding certain types of data stored and processed in computers. He said restrictions were imposed regarding transfer, dissemination, modification, and existence of various data. As applied to a shared computing system, such as Infonet, Tenkhoff said, compliance with these provisions must be a user responsibility. He said Infonet neither possessed nor desired to possess knowledge of the contents of user files stored in the Infonet system. Tenkhoff said care had been taken in the architecture of the system to keep such information from CSC employees operations personnel. Tenkhoff said it was his judgment that examination of file contents was neither practical nor ethical. He said this philosophy of design and operation was a vital aspect of the security that CSC provided its users. "Thus, legal issues dealing with privacy and the contents of files must rest solely with the user," Tenkhoff declared.

Tenkhoff said a using agency whose data falls within the provisions of the Privacy Act of 1974 must, on its own behalf, assure compliance with the law by proper design of its particular application. Tenkhoff said the user must insure that both the design and use of the particular application program have the appropriate administrative controls so that the provisions of the act may be satisfied.

While the prime responsibility rests with the using agencies, Tenkhoff said, the computer services supplier—in this instance, Infonet—also has responsibilities to provide an appropriate security environment in which the user is able to insure compliance with the Privacy Act. Tenkhoff said two key sections of the law related to the providing of a level of security commensurate with the privacy protection which is to be achieved.

Tenkhoff said that section 2(e)10 of the measure states that each agency must "Establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records." Tenkhoff said section 2(e)9 states that each agency that maintains a system of records must "Establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records."

Tenkhoff said the difficulty which confronts both the system user and the services supplier was one of interpretation. What are, he asked, "appropriate" safeguards? A review of the Infonet security features as they apply to the ability of user agencies to comply with the Privacy Act had resulted in CSC's conclusion that Infonet has provided "appropriate" safeguards, Tenkhoff said. Tenkhoff then asserted that the Stanford Research Institute audit of Infonet, although it preceded implementation of the Privacy Act, substantiated CSC's conclusion that appropriate safeguards had been realized at Infonet in connection with the Privacy Act.

Under the provisions of the Privacy Act, Tenkhoff said, the Office of Management and Budget (OMB) was assigned responsibility to formulate guidelines for compliance. Tenkhoff said OMB enlisted the assistance of the National Bureau of Standards (NBS) in the Commerce Department to prepare the guidelines. Tenkhoff said the principal documents in this regard to date were, first, Federal Information Processing Standards (FIPS) Publication 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974," and, second, FIPS-31, "Guidelines for Automatic Data Processing Physical Security and Risk Management."

Tenkhoff said FIPS-41 and FIPS-31 contained numerous useful guidelines for assessing the security of an installation and assisting in the determination of appropriate levels of security. He said Infonet had reviewed and used both documents to the extent to which the guidelines were applicable. But, Tenkhoff said, the one principal problem with the FIPS-41 and FIPS-31 guidelines is that they are oriented to computers operated by Government agencies in a dedicated environment. "Many of the particular considerations associated with commercial time-sharing systems are not discussed" in FIPS-41 and FIPS-31, Tenkhoff said. This assertion by Tenkhoff is supportive of a preliminary finding of the Senate Government Operations Committee staff, which is that Federal officials, particularly those at OMB and GSA who have security responsibilities, have neglected to provide for adequate security safeguards in connection with ADP services performed for the executive branch by commercial computer firms. The staff noted, for example, that, with the exception of contracts to commercial firms for ADP work in the national security area and other limited areas, there are no provisions for background checks on personnel employed in nondefense but nonetheless sensitive projects such as ADP activities having to do with those systems which process financial transactions leading to disbursement of public funds. As will be described later in this staff study, for instance, the committee staff could discern no consistency in Government policies regarding the hiring of persons to perform computer system programing. As an extreme illustration—one that will be described later in this report—felons incarcerated inside a Federal penitentiary were found to be working as programers for Department of Agriculture ADP projects which had to do with systems which process financial transactions leading to disbursement of public funds. It was the staff's view that if felons, several of whom were white-collar criminals and almost all of whom had relatively high recidivism rates, were programing computer systems for Federal agencies, then anyone—no matter what his or her background—would have to be, or could conceivably be, considered suitable for employment in sensitive executive branch ADP projects, either under the direct employ of the Government or on a commercial contractor basis.

It was Tenkhoff's opinion that the FIPS-31 guidelines fell short of their goal regarding the labeling and storage of personal data. Tenkhoff said FIPS-31 calls for separate labeling and storage of personal data. But, he said, the entire concept of a system like Infonet is that file contents remain unknown to operating personnel. Accordingly, Tenkhoff said, it is neither feasible nor desirable to label separately the media which contain such data.

Tenkhoff said the El Segundo computer center contains about 400 physical disks and 40,000 reels of tape. He said Infonet had no idea, nor did it wish to know, how many of these disks and tapes, if any, contain personal data. Tenkhoff said Infonet had provided a high degree of physical security for all disks and tapes. They are stored within the confines of the computer security area or in a vault at all times, Tenkhoff said, explaining that this combination of physical protective security plus the anonymity associated with multiple user files randomly located throughout the physical storage media is believed by Computer Sciences Corp. to provide a degree of protection at least equivalent and better than that of distinctly marking personal data volumes.

Tenkhoff said this illustrated the strong need for logical interpretation of law and guidelines. He said a totally rigid interpretation, in a field devoid of standards, could lead to a combination of uncertainty, unreasonableness, and ultimate high cost to the user.

The issue of cost was then addressed by Tenkhoff. "It should be well accepted that there is no system which is 100 percent secure," he said. "Given sufficient time and resource investment, any system can be compromised." Tenkhoff went on to say that the goal of proper security system design should be to make the cost of compromising the system outweigh the value of the data. He said this ideal was not difficult to articulate but that its practical realization can be difficult.

In a shared environment, he said, such considerations as cost take on an additional dimension. Needs of user applications for security vary widely, he said. Tenkhoff said the engineer developing a subroutine for performing some complex calculation probably had little concern over the security of his data and it is unlikely that it would have high value to someone else. But, Tenkhoff said, a corporation's consolidated financial data could be highly valuable to others and, in that instance, high security would be warranted. Infonet's objective, Tenkhoff said, was to provide a level of security for all users which was satisfactory for all but the most vital data. He said that these additional security options were provided for users with extremely high security requirements.

Tenkhoff said Infonet's approach to security options for extremely high security permitted the costs associated with this security to be borne only by the users requiring such features. For example, he said, if a user decided to store data in an encrypted form, he could do so. Tenkhoff said the computer resources used to encrypt and decrypt the data were charged to the user. If encryption were to be forced upon all users, then the cost to each user would be increased substantially, Tenkhoff said, adding that arbitrarily high levels of security may be achieved but high costs will accompany these increases. "Security is analogous to system reliability—achievement of the last fractions of a percent toward the absolute is accompanied by extremely high cost," Tenkhoff said.

Tenkhoff went to say that, "Security cannot be added to a system; it must be designed into it." He said if the fundamental design of the system is not sound, then increasing the investment only increases cost but it does not add security protection. Tenkhoff said that it does little good, for example, to add to the physical security of the computer area if the system can be easily compromised by a remote terminal.

Tenkhoff said he was concerned that persons with insufficient knowledge of computer technology and the problems associated with it should insist upon arbitrary security procedures in ADP systems. On this point, he explained:

> It is important that the Congress and State legislatures have a firm understanding of cost and result implications before passing additional privacy and security legislation. Such legislation must recognize the state of technology so that arbitrary measures are not enacted whose principal result would be to substantially increase the cost of computing while not materially providing any higher degree of security.

Tenkhoff concluded his paper by making two final points. First, he said, the principal security problem for Infonet today lies with the user of the service and not with the system itself. To help overcome this problem, he said, Infonet was trying to increase its security awareness and user education program. Second, Tenkhoff said, Infonet meets or exceeds the security requirements of the user applications currently being processed. Tenkhoff said that marginally increased security might be achieved in selected areas. But, he concluded, the cost would be reflected in high usage charges and would not be justified by the needs of the applications currenty being processed.

INMATES AND INFONET

The Computer Sciences Corp., owner of the Infonet computer system, issues a newsletter entitled, "CSC News." The December 1975 edition of the newsletter carried an article on page 4 with the headline, "Infonet Working 'Inside Job' at Leavenworth Federal Prison."

Datelined Leavenworth, Kans., the CSC News article said that "Prison walls are no barrier to aspiring computer programers at Leavenworth Federal Penitentiary." The article said that with the help of a recently installed Infonet terminal, prisoners hope to become "a key programing source" for the Federal Government and productive members of society at the same time.

The inmates, the article said, worked in the Federal Prison Industries, a Government corporation set up by Congress in 1934 to train inmates in useful skills and help market their services to other Federal agencies.

The article said the computer center in the prison's "school building" looked much like any other ADP facility, except that the staff wore old army uniforms and there were bars on the windows. The installing of the Infonet link at the prison was supervised by Mike Seeb, a regional branch support manager. Seeb trained the convicts on how to use the Infonet system after it was installed, the article said.

The article quoted Seeb as saying that entering the "big house" of the U.S. prison system was "a sobering experience." The article said the prison was surrounded by walls 40-feet high, 16-feet wide at the bottom and 16-feet into the ground. Seeb said that on each of his visits to the "heavily guarded structure with its 2,000 inmates," he was required to swear that he was carrying no alcohol, ammunitions, firearms or narcotics, according to the CSC News article.

The article said Seeb was then permitted to walk up shallow steps; designed to permit entry by longer term "visitors" in leg chains. Then, the article said, Seeb passed through three additional sets of guard gates whereupon he was met by an escort designated by prison officials.

During the pilot training course, which began in October of 1975, Seeb taught COBOL, a computer language, and an introduction to Infonet operating systems to four selected inmates and two civilian members of the ADP staff of Federal Prison Industries, the article said. None of the students had any experience with timesharing systems, the article said, but Seeb found the convicts "very quick to learn." The article quoted Seeb as having observed, "They are all willing to take the ball and run with it—though not too far, of course."

The article said that some unusual security arrangements were required. Seeb said that since inmates were not allowed to use a telephone, civilian employees made the client contacts, marketed prison services and handled all phone support. The article said the inmates were paid a minimal hourly wage, provided "full programing and documentation support, and implement systems on Infonet according to customer specification."

The article said Seeb had "gone beyond the call of duty" in eating in the prison mess but that Seeb was "very enthusiastic about the program" anyway. "The success of the first class demonstrates that there's a high probability the rest of the inmate programing population will also do as well," Seeb was quoted as saying. Seeb noted that there were 58 convicts in the prison ADP department at the present time.

The CSC News article said that the prison had its own computer and that using that computer the prisoners had developed about 300 accounting programs since 1972 for the U.S. Department of Agriculture's Agricultural Stabilization and Conservation Service. The article said, "Now the addition of Infonet allows them to offer their services to a much wider market." Seeb himself was quoted as saying, "We're looking forward to cooperation from other Federal Government customers and maybe commercial customers too."

The article said that the initial contract with Federal Prison Industries was made by Robert Shirey, Infonet's Federal Government Marketing Account manager for justice and transportation systems in Washington, D.C. The article said that Shirey, upon learning of the needs of Federal Prison Industries, proposed that Infonet could be used not only to train a "reliable and economical corps of programers for Federal agencies but also to market their services directly through the network."

The article said that according to Al Stober, data processing supervisor at the prison, the remote computing service had helped the inmates' business prospects in many ways. The article said system development was easier and faster "since the interactive mode of operation allows programers to correct their mistakes as they go along." "Also," the article said, "trainees now receive a much broader education in the latest programing techniques."

Stober was quoted as saying, "One of the most readily identifiable benefits of the program is on the social level. By redirecting the efforts of these men, many will be eligible for responsible data processing jobs as soon as they have completed their sentences."

BACKGROUND ON THE PRISON INDUSTRIES

On May 17, 1976, the U.S. General Accounting Office issued a report to the Congress entitled, "Examination of Financial Statements of Federal Prison Industries, Inc., For Fiscal Year 1975." The report was delivered to Senator Abe Ribicoff of Connecticut, who, as chairman of the Senate Government Operations Committee, receives all of GAO's Reports to Congress. The report, required under the Government Corporation Control Act (31 U.S.C. 841), was also delivered to the President pro tempore of the Senate, the Speaker of the House, the chairman of the House Government Operations Committee and to James Lynn, Director of the Office of Management and Budget, and Edward H. Levi, the Attorney General.

In its report on the financial statements of the Federal Prison Industries, Inc., for fiscal year 1975, GAO said the Government Corporation Control Act required the Comptroller General to examine the financial transactions of the Federal Prison Industries, Inc., (FPI).

GAO said the Federal Prison Industries, Inc., a wholly owned Government corporation created June 23, 1934, functioned within the Department of Justice under the general direction and supervision of the Attorney General. GAO said the corporation's primary function was to employ inmates in Federal prisons so as to keep them busy and, at the same time, give them an opportunity to obtain training in marketable skills. During fiscal year 1975, the corporation operated 52 industries at 23 Federal penitentiaries, GAO said.

After its examination of FPI's financial statements for fiscal year 1975, GAO auditors found their own studies of FPI, as well as those conducted by the Justice Department, to demonstrate that Federal Prison Industries' books were in order and in conformity with the Law.

GAO said the operating policies of FPI were set by a six-member Board of Directors appointed by the President of the United States. The Directors, GAO said, were appointed for indefinite terms and served without compensation. The members of the Board of Directors, at the time of the GAO report, were James L. Palmer, president, who was appointed in September of 1951 and who served as a representative of retailers and consumers; John Marshall Briley, appointed in January of 1960 and represented the Secretary of Defense; George Meany, appointed in December of 1947 and represented labor; Berry N. Beaman, appointed in January of 1954 and represented industry; William E. Morgan, appointed in May of 1966 to represent agriculture; and Peter B. Bensinger, appointed in April of 1974 to represent the Attorney General.

GAO said the Commissioner of Industries in FPI was Norman A. Carlson, the Director of the U.S. Bureau of Prisons. The Associate Director was David C. Jelinek; and the Secretary was Paul Plein, GAO said.

GAO said Government agencies are required to purchase such Federal Prison Industries products from FPI as meet their requirements and as may be available at prices not exceeding current market prices. GAO said the FPI Board of Directors had established the policy that prices for FPI products could not be materially below current market prices.

In fiscal year 1975, GAO said, FPI's 52 industries in 23 Federal prisons manufactured goods or provided services that included gloves, brushes, brooms, and automatic data processing and printing services. GAO said the total employment for the fiscal year averaged 5,207, or about 22 percent of the total inmate population.

GAO listed sales, profits, losses, and average inmates employed for each of the FPI industries according to the goods or services sold during fiscal year 1975. In the automatic data processing field, GAO said, three Federal prisons were selling services. The prisons were the Federal penitentiaries at Alderson, W. Va.; Fort Worth, Tex.; and Leavenworth, Kans.

In sales for 1974, Alderson showed a record of $318,357 and for 1975, $296,885. Profits in 1974 were $56,692 and $92,208 in 1975, GAO said. An average of 49 convicts were employed at Alderson during this period.

At the Fort Worth facility, where 31 convicts were employed, GAO said, prisoners registered sales of $73,830 and $103,138, respectively, for fiscal years 1974 and 1975. Profits in this pursuit at Fort Worth were $4,031 in 1974 and $30,014 in 1975, GAO said.

Leavenworth convicts had sales of $301,936 in 1974 and $351,493 in 1975, GAO said, adding that profits at Leavenworth in 1974 were $36,629 in 1974 and $48,919 in 1975. GAO said 44 inmates worked on ADP projects at the FPI program at Leavenworth during this period.

INFORMATION ALLEGING TAX FRAUD

In May of 1976, the staff of the Senate Government Operations Committee developed information indicating that inmates at the Leavenworth Federal penitentiary had allegedly perpetrated a fraud on the Internal Revenue Service for a large amount of money.

On May 19, 1976, the committee staff submitted a memorandum to Senator Ribicoff in which they said that information had come to them alleging that a group of convicts currently serving time at Leavenworth had conceived a complex scheme to defraud the Internal Revenue Service by beating the audit and computer systems. The size of this alleged group and the identity of the individuals reportedly involved were not known. However, the committee staff said, the perpetrators of the alleged scheme were thought to have been convicted and incarcerated for crimes that included white collar violations.

The alleged group of imprisoned tax violators reportedly had devised a scheme whereby they created fictitious companies and businesses, the committee staff said in the memorandum to Senator Ribicoff. Complex tax returns were allegedly created for these businesses showing pages of deductions and other expenses, the committee staff said. The returns were so detailed as to "beat" the tolerance levels set on IRS computers. "In other words," the committee staff said, "the returns would not normally disturb the computer 'audit' alert which automatically picks up a deduction which is out of the ordinary."

Other aspects of the information provided to the committee staff included unsupported allegations that the scheme was facilitated by the fact that Federal prisoners had full mailing privileges at Leavenworth and that incoming and outgoing mail was not censored by prison officials; that the alleged scheme was accidentally uncovered by a low level IRS computer clerk who decided to query the IRS computer in connection with multiple filings and multiple disbursements of refunds, that is, numerous checks going to the same address; that IRS criminal investigators were making an inquiry into the information uncovered by the low level IRS clerk; and that an intensive investigation into this alleged scheme was being conducted by special agents of the IRS, the U.S. Postal Inspection Service, the Bureau of Prisons and the U.S. Attorney's Office, Kansas.

In the memorandum, the committee staff said they had information indicating that the investigation of the alleged scheme was being handled "very discreetly." Officials of the affected agencies were said to be concerned about the embarrassment to the agencies involved and various prison programs reportedly abused by the alleged group of convicts. To date, the committee staff said, some of the money had been recovered. But, the staff said, prospects for additional recovery of the IRS refunds were reportedly slight because most of the money had already been diverted into secret bank accounts.

Upon receipt of the memorandum, Senator Ribicoff directed that this information be made available immediately to the appropriate authorities at the Bureau of Prisons and the Internal Revenue Service. Such arrangements were made at the chairman's direction.

JUNE 7, 1976 MEETING

Moreover, on Monday, June 7, 1976, at 10 a.m. a meeting was held in Senator Ribicoff's office in the Russell Office Building. The meeting was attended by Senator Ribicoff; IRS Commissioner Donald C. Alexander; Assistant IRS Commissioner for Accounts, Collection and Taxpayer Service Robert H. Terry; Norman A. Carlson, Director of the Bureau of Prisons; Assistant Director David C. Jelinek; Malcom O. Campbell, Jr., Senator Ribicoff's administrative assistant; and committee staff.

It was explained at the meeting to the representatives of the executive branch agencies that the Senate Government Operations Committee was engaged in a preliminary staff investigation of problems associated with computer technology in Federal programs and private industry and that in the course of this preliminary staff investigation the information regarding the alleged income tax fraud scheme had surfaced and that the committee was hopeful that IRS and the Bureau of Prisons would work with committee investigators in carrying out the congressional oversight function in this matter. There was general agreement among the participants in the meeting that cooperation between the committee and the executive branch was not only possible and agreeable but also desirable. Executive branch representatives at the meeting said they would immediately inquire into the alleged convict scheme.

Senator Ribicoff directed the staff to expand its preliminary investigation to include an examination of the Leavenworth situation. The staff then set out to examine (1) the nature and scope of any scheme on the part of the inmates at Leavenworth to defraud the Internal Revenue Service by beating the computerized system of selecting tax returns for audit; (2) any possible weakness in the IRS computer operations with respect to dealing with the problem of fraudulent filings and refund schemes; (3) the operations of the computer training and rehabilitation project at Leavenworth with emphasis on the criminal background of those being trained and any potential irregularity or misuse of this program by inmate programmers from a security standpoint; and (4) any possible connection between the alleged fraudulent scheme to defraud IRS and the computer training project at Leavenworth.

BACKGROUND ON INMATES

The committee staff looked into the backgrounds of the convicts involved in the computer programing project at Leavenworth. From 1972 until June of 1976, 157 convicts participated in the ADP program at Leavenworth. Of the 157 convicts, the Bureau of Prisons was able to provide statistical data on 142 of the prisoners. This information was provided the committee by the Bureau of Prisons in a document dated July 7, 1976, entitled "Longitudinal Study of ADP Industry Participants—U.S.P. Leavenworth, June 1976."

The Bureau of Prisons document indicated that of the 142 convicts on whom documentation was available 43 were still active in the program; 51 inmates were still incarcerated at Leavenworth or elsewhere; and 48 convicts had been released from custody. Of the 48 released, 6 had been returned to prison for violations of the law. One of these six, the Bureau of Prisons report said, was imprisoned for a computer-related crime. In turn, of the 48 convicts released from prison after having received training in computer programing and having worked in FPI projects under contract to the Agriculture Department, 24 ex-convicts had found employment in the ADP field in civilian life outside the prison.

For purposes of classification the Bureau of Prisons characterized the criminal background of the 142 participants on whom documentation was available. Thirty-eight convicts or 27 percent of the 142 participants were classified as white collar criminals whose offenses included convictions for crimes such as fraud, embezzlement, forgery, and interstate transport of stolen securities.

The Bureau of Prisons report said the remaining 104 convicts, or 73 percent of the 142 participants, were divided into 3 categories according to the degree of violence attendant to the crimes for which they had been convicted. Sixty-nine of these were classified as being in the most violent group, their crimes including murder, kidnapping, or bank robbery. Eighteen participants were classified as "property crime" violators whose offenses included theft, larceny, or burglary. Seventeen of the participants were found guilty of drug-related offenses.

The Bureau of Prisons informed the Senate Government Operations Committee that the only criteria used for admission to the computer program were, first, a desire on the part of the convict to learn ADP skills; and, second, an intelligence quotient or IQ of 110 or more, as determined by preadmission testing. No evaluation of the inmate's reason for being in prison was made as to whether or not he should be admitted to the ADP project. The convict's criminal background, whether it be organized crime, white collar crime, violent crime, or drug-related crime, did not disqualify him from participation in the training program or subsequent computer programing projects for other Federal agencies such as the U.S. Department of Agriculture.

The Bureau of Prisons said that of the 142 convicts on whom documentation was provided, 114 convicts entered the ADP program as trainees. Of the 114 trainees, 103 went on to become computer programers. Eleven dropped out or were still in training, the Bureau of Prisons report said. In addition, 16 convicts entered the project as ADP support personnel such as clerks and keypunchers. Twelve of the 142 convicts received training which the Bureau of Prisons could not account for.

As of June 15, 1976, 45 inmates at Leavenworth were identified by the Bureau of Prisons as working for Federal Prison Industries in providing computer programing services for Federal offices. The committee staff obtained information from the Bureau of Prisons on the criminal backgrounds of the prisoner computer programers. The Bureau of Prisons gave the committee individual criminal background files, commonly known as "rap sheets," on the inmates as well as criminal background records from the National Crime Information Center (NCIC). The following description of their arrest and conviction records will not include their names, FBI numbers or dates of birth. The convicts will be identified by number in chronological order. Several of the convicts can be characterized as "career criminals," according to a definition used by the Law Enforcement Assistance Administration of the Department of Justice. A career criminal, LEAA says, is a person who has had five or more felony arrests and two or more felony convictions.

Convict No. 1 was convicted October 6, 1970, for bank robbery and sentenced to 15 years in prison. He was sentenced to 1 additional year to run concurrently, after escaping from custody. Convict No. 1 has a record of 12 arrests and 12 convictions. His convictions include five for burglary, one on a drug charge, four for other drug charges and one each for an unlawful weapons offense and flight to escape prosecution.

Convict No. 2 was convicted April 12, 1973 and sentenced to 15 years in prison for kidnaping. Convict No. 2 was arrested on this charge 3 days after he was released from prison in Oklahoma where he was serving a 3-year sentence for burglary and escape by force. Convict No. 2 has been arrested eight times and convicted six times. His convictions include one violation of the Uniform Code of Military Justice and kidnaping, robbery, burglary, stolen vehicle, flight to escape prosecution and another offense not recorded.

Convict No. 3 was sentenced February 18, 1972 to 15 years imprisonment for armed robbery. He was arrested but not convicted in connection with another instance of armed robbery.

Convict No. 4 is serving two life sentences for first and second degree murders on an Indian reservation. He was convicted on these charges on August 4, 1966 and June 5, 1968, respectively.

Convict No. 4 was convicted previously for assault with a dangerous weapon on an Indian reservation and given a sentence of 3 years probation. Convict No. 4 is on the special offenders list at Leavenworth. This list is also known as the central inmate monitoring program. The special offenders list contains the names of inmates who are most carefully watched by prison authorities due to either connection to organized crime, notorious criminal behavior, inclination to escape, specially violent acts or because they testified against other suspects in Federal trials and may, therefore, be targets of retribution by other inmates.

Convict No. 5 is serving a 15-year sentence for armed bank robbery, having been convicted January 31, 1975. He has been arrested seven times and convicted for homicide twice, robbery twice, and attempted larceny once. Convict No. 5 was, prior to his incarceration at Leavenworth, convicted for murder in Wisconsin and sentenced to two life sentences. He escaped from a State hospital as well. Convict No. 5 is on the special violators list.

Convict No. 6, on July 30, 1971, was convicted of bank robbery and escape and sentenced to 27 years in prison. Of his 13 arrests, he has been convicted of robbery twice, fraud once, and flight to escape prosecution three times.

Convict No. 7 was convicted in June 1973 of armed bank robbery and conspiracy and received a 12-year sentence. His convictions include assault homicide, attempted robbery, robbery, burglary, and "public order crimes."

Convict No. 8 was sentenced to 25 years in prison for bank robbery in July 1973. His convictions include attempted murder, and three robberies.

Convict No. 9 was convicted December 14, 1973 for bank robbery with the use of a dangerous weapon. He received a 20-year sentence.

Arrested nine times, he has been convicted for three robberies, two larcencies and one weapons offense.

Convict No. 10 was convicted in March 1973 and given a 9-year sentence for bank robbery. Having been arrested five times, convict No. 10 has been convicted for three robberies and one larceny.

Convict No. 11 was sentenced to 12 years in prison on May 14, 1971 for bank robbery and conspiracy. On November 14, 1972, he was sentenced to 5 more years for escape from prison. At the time of his transfer to Leavenworth, convict No. 11's sentence was a total of 17 years and 3 months. Convict No. 11 has been convicted for robbery, two burglaries, a larceny, a forgery, and counterfeiting offense and four illicit drug violations. He is on the special offenders list.

Convict No. 12 was convicted December 12, 1969 and sentenced to 7 years in prison for interstate transportation of forged securities and several Dyer Act violations. Of 13 arrests, convict No. 12 has been convicted of a larceny, stolen cars three times, forgery, counterfeiting twice and four frauds.

Convict No. 13 was sentenced to 15 years in prison for bank robbery in March 1971. In August 1972 he was sentenced to 8 years by State authorities; the 8-year term was to be served concurrently with his Federal incarceration. He has nine arrests and seven convictions, including three robberies, three burglaries and one flight to escape prosecution.

Convict No. 14 has the highest recidivism rate of any of the participants in the Leavenworth computer program. In February of 1972, he was convicted and sentenced to 10 years in prison for interstate transportation of forged securities. Convict No. 14 has been arrested 25 times and has been convicted 16 times for offenses that include attempted robbery, robbery, 2 assaults, burglary, larceny, 6 forgery and counterfeiting offenses, 1 fraud, 1 embezzlement, 1 obstructing police, and 1 traffic violation.

Convict No. 15 was sentenced to Leavenworth in February of 1973, having been convicted for conspiracy to distribute heroin. His term is 11 years. He was arrested three other times but this is his only conviction.

Convict No. 16 had, as of July 1, 1970, a consolidated sentence at Leavenworth of 35 years for convictions on three counts of bank robberies. His record includes five arrests and convictions for robbery and two car thefts.

Convict No. 17 was convicted November 15, 1972, and received a 15-year sentence for extortion and stealing cars. He was arrested 17 times and convicted of robbery, extortion, larceny, 3 car thefts, flight to escape prosecution, and 1 traffic offense.

Convict No. 18 was sentenced to 20 years in April 1971 after being convicted of armed robbery. His criminal record consists of two arrests for armed robbery and two convictions.

Convict No. 19's only arrest resulted in his present 10-year sentence. He was found guilty of armed robbery.

Convict No. 20 was convicted and sentenced to 16 years in prison November 1, 1974. Of five arrests, he has three convictions, for armed robbery, burglary, and a traffic offense.

Convict No. 21 is serving a 20-year sentence for armed bank robbery after his November 19, 1974, conviction. Arrested eight times, he has been convicted for aiding and abetting a robbery, two robberies, assault, and embezzlement.

Convict No. 22 was sentenced February 18, 1971, to a 20-year term for armed bank robbery. He was arrested 12 times and convicted for robbery, car theft, a weapons offense, 6 burglaries, and 3 larcenies.

Convict No. 23 pleaded guilty to several counts of bank robbery and received a 25-year sentence. It was reduced to 20 years on January 1, 1974. Convict No. 23 was arrested and convicted four times for armed robbery.

Convict No. 24 was sentenced March 3, 1975, to 20 years in prison for bank robbery. As a result of eight arrests, he was convicted five times, for three robberies, a burglary, and attempted flight to escape prosecution.

Convict No. 25 was convicted September 5, 1973, and sentenced to an 8-year term. The sentence was consolidated, representing convict No. 25's involvement in three separate cases involving conspiracy to receive and transport stolen vehicles in interstate commerce. Convict No. 25 has been arrested 18 times and his 10 convictions include 2 burglaries, 3 larcenies, 2 obstructions of justice, and 1 each of conspiracy to steal a car, stealing a car, forgery, counterfeiting, and "property crimes."

Convict No. 26 was convicted in April 1973 and given a 15-year sentence for bank robbery. In 10 arrests, he has been convicted in three robberies, and for assault, burglary, and stolen vehicle.

Convict No. 27 was convicted in July 1971 and sentenced to 25 years in prison for armed bank robbery. Arrested 12 times, convict No. 27 was convicted for 3 robberies and for attempted assault, burglary, attempted larceny, and larceny. Convict No. 27 is on the special offenders list at Leavenworth.

Convict No. 28 was sentenced in May 1974 to a 15-year term for bank robbery. While he has been arrested 13 times, his only other conviction was in a fraud case. Convict No. 28 is on the special offenders list.

Convict No. 29 received a 17-year sentence in February of 1971 after his conviction for conspiracy to sell and possess heroin. He has been arrested three times in his life, each arrest related to narcotics violations. Convict No. 29 is on the special offenders list at Leavenworth.

Convict No. 30 was convicted and sentenced to 30 years in prison for armed bank robbery in December 1974. When convict No. 30 committed the armed bank robbery, he was a parole violator from the State of Oklahoma where he had been convicted and sentenced to 20 years for armed robbery. Convict No. 30 was arrested three times and his convictions include three robberies and one burglary.

Convict No. 31 was convicted in June 1974 for a series of parole violations as a result of previous convictions for fraud by wire. He was sentenced to 6 years. His criminal record includes 14 arrests and 4 convictions—3 frauds and 1 obstruction of justice.

Convict No. 32 is serving a prison term at Leavenworth of undetermined duration. The sentence was handed down in August 1971 when he was found guilty of bank robbery. He has been arrested five times and convicted of larceny, robbery and burglary twice.

Convict No. 33 pleaded guilty June 18, 1973, to bank larceny charges and was sentenced to 10 years in prison. Convict No. 33 has been arrested 15 times and his convictions include 2 robberies, an assault, a burglary, a larceny and car theft.

Convict No. 34 in June 1970 was sentenced to 55 years in prison for bank robbery. He has been arrested seven times and his eight convictions include two robberies, two burglaries, stealing a car, theft of property, illegal gambling and obstruction of justice. Convict No. 34's name is on the special offenders list at Leavenworth.

Convict No. 35 was convicted and sentenced to 6 years in prison in February 1973 for extortion. Arrested nine times, he has been found guilty six times, for extortion, burglary twice, attempted larceny, damage to property and flight to escape prosecution.

Convict No. 36 was convicted in March 1975 of falsely altering and forging a U.S. Treasury check. Four years in prison was his sentence. Convict No. 36 was given a 5-year sentence in 1971 for interstate transportation of forged securities and was paroled in June 1974. Convict No. 36 was arrested on 18 occasions and has 8 convictions, which include 4 forgery and counterfeiting offenses, 2 stolen property crimes, a "public order crime" and conspiracy to commit a burglary.

Convict No. 37, in June 1975, was given a 15-year sentence for armed bank robbery and escape from Federal custody. In 1972, convict No. 37 was sentenced to 15 years in prison in Oregon for robbery in the first degree. Convict No. 37 has a total of 11 arrests and 6 convictions, for robbery twice, car theft and 3 flights to escape prosecution.

Convict No. 38 is in Leavenworth serving a 20-year sentence for selling heroin. His conviction was in April 1971. Convict No. 38 was arrested four times and convicted for burglary, three drug violations, drunkenness and disturbing the peace.

Convict No. 39 is in Leavenworth Penitentiary serving a 10-year term for his July 1974 conviction for homicide as an accessory after the fact in the murder of a Federal officer. He has been arrested four times but his only conviction is the one for which he is presently serving time. Convict No. 39 is on the Leavenworth special offenders list.

Convict No. 40 was convicted in October 1972 and given a 40-year sentence for armed bank robbery. With two arrests in his past, convict No. 40 has been convicted of the armed bank robbery charge and burglary.

Convict No. 41 began a 20-year sentence February 29, 1972, for bank robbery. He has been arrested seven times and has convictions for two bank robberies, one weapons offense, an attempted burglary, and a violation of the Uniform Code of Military Justice.

Convict No. 42 is in Leavenworth following a December 14, 1973 conviction for interstate transportation of a stolen aircraft and bond jumping. Ten years is the length of his sentence. Among his 12 arrests are convictions for larceny, 2 car thefts, 2 forgery and counterfeiting offenses, 2 frauds, a stolen property offense, and an obstruction of justice violation.

Convict No. 43 was sentenced to 20 years in June 1966 after his conviction for armed bank robbery. He was paroled to the U.S. Marshals Service but was subsequently sentenced to a 5- to 25-year term for kidnaping and extortion. Convict No. 43 is presently in

Leavenworth serving a consolidated sentence of 20 years. He has been arrested seven times and his four convictions are for kidnaping, robbery and forgery and counterfeiting twice.

Convict No. 44 was convicted July 7, 1975, and sentenced to 7 years for interstate transportation of bogus securities. He has been arrested 34 times and his 12 convictions are for 2 burglaries, a larceny, 5 forgery and counterfeiting offenses, a fraud, an obstruction of justice, and 2 weapons offenses.

Convict No. 45 began serving a 10-year sentence for bank robbery in April 1974. At the time of his last arrest he was on parole following conviction, with a resulting 15-year sentence for armed robbery. Prior to that, convict No. 45 had also been discovered to have violated parole after a 15-year sentence for conviction of breaking and entering. Arrested six times, convict No. 45 has convictions that include conspiracy to commit robbery, two robberies, and a burglary.

The staff of the Senate Government Operations Committee noted earlier in this staff study that Bureau of Prisons officials said 43 inmates were, as of this writing, participating in the Federal Prison Industries ADP program at Leavenworth. However, upon the committee's request for criminal background records, or "rap sheets," on the participants, the Bureau of Prisons provided data on 45 convicts.

The Senate Government Operations Committee staff made a criminal record profile on the participants in the Leavenworth computer programing services project. The staff said that of the 45 prisoners taking part, 41 of the participants could be classified as recidivist criminals in that they had been convicted of at least 2 felonies, and had a least 5 felony arrests.

The committee staff's profile of the prisoner programers showed that, with the exception of one participant who is serving a life sentence and another whose sentence is unknown, the average current sentence per participant is 16.9 years. It was the staff's conclusion that, taking into account current parole practices exercised in Federal prisons, it is likely that the average prisoner working in the FPI computer services program will serve about 5 years actual prison time before being released on parole, assuming no new violations should be initiated while the individual prisoner is incarcerated. Independent inquiry by the Senate Government Operations Committee staff indicated that convicts are usually eligible for parole after serving one-third of their sentence, unless the sentence contained stipulation to the contrary.

The staff of the Senate Government Operations Committee also noted that the ADP participant profile at Leavenworth showed that the average prisoner computer trainee at Leavenworth had been arrested 9.04 times and convicted 5.66 times.

ADP TRAINING PROGRAM

Along with reviewing the criminal backgrounds of the prisoner computer programers at the Leavenworth penitentiary, the committee staff also examined the training and rehabilitation program they are engaged in. The staff found that the computer facility at Leavenworth is not limited to the training of convicts in ADP programing and other related skills for purposes of rehabilitation. Once the convict has been trained to a certain level of proficiency in ADP skills, he can participate in writing and testing actual working programs for ongoing Federal Government projects as a part of the Federal Prison Industries' ADP programing services industry at Leavenworth.

The FPI programing services industry has contracted with Government agencies, and provides programing services, for a fee consistent with rates charged by commercial firms. The fees charged by the programing industry at Leavenworth create a profit for the overall Federal Prison Industries, Inc., program. Inmate programers at Leavenworth are paid about 50 cents an hour.

In documentation provided the committee by the Bureau of Prisons it was noted that computer programing vocational training began at the U.S. Penitentiary, Leavenworth, Kans., in 1963 under the prison's education department.

In July 1964, the first equipment was installed, enabling inmates to test their programing efforts on an actual computer. John Willingham, the warden at the time, said, "Our goal is to help our men prepare for their tomorrow. Data processing is one of such programs that, when combined with judgment in its application, will lead directly to that goal."

The Bureau of Prisons documentation indicated that profits realized by the Bureau's Federal Prison Industries, Inc., were sufficient to invest more money into the computer training program at Leavenworth. By 1970, two full-time employees had been hired to teach and administer the ADP vocational program. The equipment had been upgraded to a "modern third generation computer" and formal classes were conducted for students permanently assigned to the school, the BOP documentation said. Joseph A. McKinley, supervisor of education at the time, said the goal of the training was to produce 30 computer operators and 15 computer programers a year.

In 1973, Federal Prison Industries, Inc., established the Computer Programing Industry at Leavenworth "to provide an open-ended asset to the existing vocational training program," the Bureau of Prisons said, explaining, "The industry was added allowing the number of inmate participants to double, and providing an opportunity for the inmate to maintain and better his skills upon completion of the training until his release."

Establishment of the Computer Programing Industry followed the signing of a contract between FPI and the U.S. Department of Agriculture (USDA) for ADP programing services.

The Bureau of Prisons indicated that since 1972 the Computer Programing Industry of FPI had written 370 computer programs for the U.S. Department of Agriculture and the Bureau of Prisons. The Bureau said revenues received had been large enough to lead FPI officials to estimate that their original investment in Leavenworth ADP work would be reimbursed by December of 1976. BOP also noted that the Leavenworth computer industry of FPI had registered a 15-percent net profit over all operating costs "and recent market studies indicate that a successful future is assured."

HERBERT BANNERMAN SPEECH

On May 14, 1973, Herbert Bannerman, then a project leader of the Federal Prison Industries computer center at Leavenworth, gave a speech in San Diego before a conference of NCR computer users.

In the speech, a copy of which was given the committee by the Bureau of Prisons, Bannerman described the computer training program at Leavenworth.

Terming Leavenworth an "old Bastille-like" prison, Bannerman said the penitentiary had 2,000 inmates and a staff of about 400 employees. The average inmate, he said, was 35 years old, had an IQ of 106, was serving a sentence of about 10 years, and had "probably done time previously at other Federal and/or State institutions."

The prison's first computer was a used UNIVAC purchased in an excess Government property disposal sale, Bannerman said. From the old UNIVAC, he said, the prison moved to an IBM 407 accounting machine and in 1968 an IBM 1130 was installed. "The training was quite informal learn-by-reading-manuals-then-try-to-do-it," Bannerman said. "These early inmates had no professional help available with the exception of occasional short visits by site reps."

With the limited training, it was "amazing" that progress was achieved but the inmates did move forward, Bannerman said. He said the inmates at Leavenworth were given the task of maintaining the educational reporting system for the entire Bureau of Prisons. In 1969, he said, the prison installed an NCR Century 100 computer. In the summer of 1970, the first of six ADP employees was hired and in March of 1971 an NCR Century 200 computer was purchased, Bannerman said.

Popular as the ADP training program had become at Leavenworth, several inmates who wanted to participate could not afford to because they were not paid to work with the computer, Bannerman said. He said many convicts need money for commissary items because their families do not give them assistance. In turn, the inmates get paying jobs within the prison, frequently for FPI. Once FPI took on the computer project at Leavenworth, contracts were signed with the Agriculture Department and the Bureau of Prisons, thus enabling FPI to pay the prisoners about $40 a month.

Commenting in his May 1973 speech on what the future held for Leavenworth ADP industry, particularly regarding the prison's relationship with its biggest computer service customer, the Agriculture Department, Bannerman said, "The Department of Agriculture [computer center] system will be headquartered in Kansas City. It is going to be the second or third largest computer system in the country, with 10–20 billion bytes of online storage. We are very excited about this program. Training on a system of this magnitude will give the trainees an opportunity impossible to match elsewhere. As a matter of fact, the Department of Agriculture has expressed an interest in hiring some of our trainees."

Bannerman went on to say:

> The most important question about any attempt at rehabilitation is its degree of success. We know that our training is very successful because we are able to keep in touch with a good percentage of our graduates. At the present time we know of 18 locations where our graduates of the last 2 years are working. Five of these men have worked for NCR as site reps. Two have accepted better jobs with NCR users. One man is teaching programing to blacks in a Cleveland ghetto area. We have ex-inmates working in both Mexico and England. One man is now working as a programer in a steel

CONTINUED

1 OF 4

> plant where he was a janitor prior to incarceration. At least two of our graduates are now data processing managers. Thus far, none of the men have been returned to custody. We think that our record is pretty good and I for one am actually proud of our men who are working out on the streets today. As a matter of fact, one man, who is not quite 2 years out of our program, is attending this conference today. Our program is so successful, thanks largely to the excellent support given to us by NCR. A couple of years ago NCR made a corporate commitment to assist our program. As a result of this we can normally arrange a job interview in any location in the country when one of our trainees is discharged.

To qualify for the 1-year ADP training course that is preparatory to working for the FPI computer industry, a convict must have a high school diploma or the equivalent of one, his IQ should be 110, his age at projected time of release should not be over 40 and he should have about 3 years to serve to complete his sentence, Bannerman said, adding, "we see no reason to spend our time training a 'lifer' ". The convict must also score a minimum grade of 40 on the IBM computer aptitude test, Bannerman said.

Once a prisoner has met these requirements, Bannerman said, he is then considered for selection by a "classification team" composed of psychologists, sociologists and penologists. The classification team receives a "complete record" of the prospective trainee, Bannerman said. If a psychological or medical impediment is detected by the team, Bannerman said, the convict is not allowed to become a trainee. Owing to this selection process, Bannerman said, the ADP program dropout rate was very low.

Bannerman said the curriculum in the Leavenworth ADP training program was designed to achieve two purposes. The first mission, he said, was to train inmates in ADP so that they can do competent application programing for the Agriculture Department in the time between their training and release. Second, the curriculum was set up to prepare the convict to find a job when he leaves prison. In addition, Bannerman said, the primary focus of the training is to graduate computer programers, not operators. "In the past 2 years," he said, "all of our trainees have gone directly into programing."

Educational services to supplement the ADP training in the prison are provided by Highland, Kans., Junior College and Kansas University located in Leavenworth. Highland JC gives an associate of arts degree to prisoners who qualify, Bannerman said. Courses offered by the junior college and the university include three classes in computer science and selected classes in mathematics.

Bannerman said the prisoners are highly motivated as students. "They work so zealously it is rather hard for an outsider to believe," Bannerman said. Employers who had hired ex-convicts from the Leavenworth ADP program had remarked to him, "I can't believe a person can attain that degree of skill in only one year," Bannerman said.

Bannerman said:

> However, when you consider that many of our men actually put in a 14-hour day, then write and work on programs in their cells during the weekends and any other spare time, it is not hard to understand their competence.

Bannerman added:

> You hear a great deal about how the computer is helping various types of businesses become more efficient. Yet, here is a use of the computer that no one ever dreamed of. It has proven to be a successful tool in rehabilitation. Most of these men were literally on their last legs, yet the computer has proven to be as good a tool in rehabilitation as any that has been found.

FPI PROVIDES AGRICULTURE SERVICES

The Senate Government Operations Committee staff learned that since 1972 the ADP Programming Services Industry at Leavenworth under contract to the Department of Agriculture had written more than 300 accounting-related programs for USDA's Agricultural Stabilization and Conservation Service (ASCS).

The ASCS computer facility in Kansas City, Mo., is directly tied to the Programing Services Industry at Leavenworth penitentiary. The ASCS computer facility in Kansas City supports the payment of Federal funds in the soil bank program, the Commodity Credit Corporation (CCC) and about 20 other projects which distribute funds for agricultural disaster assistance.

Operating in support of the CCC, the soil bank and the agricultural disaster assistance programs, the ASCS computers account for the payment and accounting of about $4 billion a year.

The computer-trained inmates at Leavenworth write the accounting programs for the agricultural programs under the supervision of both Federal Prison Industries civilian computer personnel at Leavenworth and ASCS personnel in Kansas City,

Inmate programers at Leavenworth also provide programing services for the Bureau of Prisons itself. These programs relate to the movement and custody of all Federal prisoners in the U.S. prison system and certain accounting, budgeting, and payroll projects for the BOP. In addition, the inmate programers at Leavenworth provide an unspecified programing service for the National Endowment for the Humanities.

The Senate Government Operations Committee staff learned that Federal Prison Industries, Inc., wished to be given more computer programing business by the Federal Government. In pursuit of that goal, the General Services Administration (GSA) issued a regulation making Federal Prison Industries a mandatory supply source for ADP services. The regulation is known as Federal Procurement Regulation, or FPR, 1–5.402. It was issued December 2, 1974. FPR 1–5.402 is designed to require Federal agencies needing ADP services to first consider giving the contract to Federal Prison Industries. GSA's position is that its regulation in this regard has the effect of giving Federal Prison Industries a priority over private industry for keypunch and programing services.

In October of 1975, the Leavenworth computer facility was connected to the Infonet system. Infonet is a privately owned time-sharing system. In dollar volume, Infonet is the largest private contractor the Federal Government does business with. The connection between the prison and Infonet came as the result of a contract entered into by

Infonet's parent firm, the Computer Sciences Corp. of El Segundo, Calif., and the General Services Administration.

By late 1975, the Programing Services Industry of Federal Prison Industries, Inc., was moving to expand its operations and revenues by having as customers as many Federal agencies as it could accommodate. The Programing Services Industry of FPI now had the use of not only the computer facilities at Leavenworth but also remote terminals to Infonet and IBM equipment at the Department of Agriculture's Kansas City Computer Center (KCCC).

IRS, BUREAU OF PRISONS PROVIDE DATA

Once the committee staff had obtained information on the criminal background of the prisoner programers at Leavenworth and on the nature and scope of the ADP training program and industry at the prison, the staff then sought to evaluate the allegation it had received that inmates had organized a scheme to defraud IRS. The alleged scheme was reportedly initiated by inmates who, having learned how to avoid detection by IRS computers, filed tax returns that generated refund checks. The alleged scheme reportedly included the sending of many fraudulent tax returns attested to by fictitious W-2 forms and business records.

On June 14, 1976, committee staff went to Kansas. In Kansas City on June 15, they contacted Edwin Johnson, U.S. Attorney, District of Kansas, and Assistant U.S. Attorney James Pusateri.

Johnson said that his office andthe IRS were investigating information concerning a possible scheme to defraud IRS by inmates at Leavenworth. Johnson said that the IRS office in Kansas City, Kans., had prepared a nine-page memorandum for IRS Commissioner Donald C. Alexander.

In the memorandum, Johnson said, the IRS Kansas City office had explained the nature of the investigation and the problem of multiple file schemes.

Johnson said that his office had recently returned an indictment against an inmate at Leavenworth for a false filing and refund scheme. Johnson identified the inmate as Frank E. Ready.

James Pusateri, when interviewed, provided some details on the *Ready* case. Pusateri said that the IRS Intelligence Division had received an anonymous letter from Leavenworth in which allegations were made concerning the reported false filings of 600 tax returns which allegedly generated IRS refunds of about $6 million. Pusateri said he thought the anonymous letter probably had been written by Ready himself in an attempt to build a defense. Pusateri was skeptical of the accuracy of the contents of the letter. But, he said, IRS was investigating it anyway.

Pusateri was concerned about the possibility that the Senate Government Operations Committee's preliminary staff investigation would be prejudicial to his prosecution of Ready. He requested that during the staff's forthcoming visit to Leavenworth that no effort be made to interview Ready. The Ready trial was scheduled to begin in late June. The staff agreed not to seek to interview Ready.

Pusateri said he had no conclusive evidence to indicate that any reported scheme to defraud IRS was linked to the computer training and rehabilitation program at Leavenworth.

Robert McMillan, an IRS Intelligence Division supervisor assigned to the Kansas district, was leading the investigation of Frank Ready and other related investigations. McMillan was on travel June 14 and 15. In his absence, committee investigators contacted Al Hunter, Chief of IRS Intelligence for the Kansas district. Hunter confirmed the existence of the nine page memorandum outlining what was then known of reported efforts by Leavenworth inmates to defraud IRS. Hunter said release of the report to the Government Operations Committee would have to be made from Washington.

On June 16, 1976, the committee staff interviewed three officials at the U.S. Penitentiary, Leavenworth—Charles Benson, the warden; Hal Hopkins, the superintendent for Federal Prison Industries, Inc., at Leavenworth; and Bealer Gausz, an FPI employee who supervised the computer services operation at Leavenworth.

Benson said he was familiar with the Ready case but knew of no other reported involvement by inmates in the filing of false tax returns.

Bealer Gausz said security controls at the prison made it impossible for the prisoner programers to perpetrate a computer fraud. Gausz said that the prison was no longer connected to Infonet. He said that to his knowledge there was no connection between the Ready case and the prison computer program.

June 16, 1976 was a Wednesday. Warden Benson also noted that this was his second day on the job, having reported to his new position on the 15th.

On July 7, 1976, Norman Carlson, Director of the Bureau of Prisons, sent the committee a report entitled, "Longitudinal Study of ADP Industry Participants—U.S.P. Leavenworth 1972–June 1976." This report is the official response of the Bureau of Prisons regarding the committee's examination of the ADP project at Leavenworth. Pertinent portions of the report are as follows:

> 1. *Scope of the Study.* Of the 157 inmates who entered the program from its beginning to June, 1976, 142 could be analyzed in the time available. Documents for 15 others who departed in the early 70s were not readily available.
>
> Criminal history data was provided by NCIC/CCH; other data came from official USP Leavenworth files, and from contacts with employers.
>
> 2. *Summary.* Of the forty-eight participants released, twenty-four (50%) found jobs in the ADP field. This compares favorably with published reports of the Office of Education, which reveals that only 68% of VT [vocational training] graduates in the nation as a whole obtain jobs in their field of training.
>
> When one considers that the Leavenworth releasees have a history of unstable employment, and the stigma to overcome of being ex-offenders, the success rate becomes especially impressive.
>
> The prior criminal histories do not appear to be significant in determining success. Seventy-one percent of the white collar releasees found ADP employment, but so did sixty-seven percent of those convicted of property crimes.

> Twenty-one percent of the white collar releasees have been returned; fifteen percent of releases convicted of violent crimes have been returned. Those in the other two categories are still free.
>
> The only reported case of a computer-related crime was allegedly perpetrated by a participant in the violent offense category.
>
> *Recommendation.* According to the latest Occupational Outlook Handbook Quarterly Update (Spring 1976), computer programming will continue to be a desirable occupation during the next decade. Thousands of jobs will become available; persons with experience will have the best chance.
>
> Programmers' salaries are nearly double that of other industry non-supervisory workers. The program at Leavenworth, therefore, provides experience in a highly paid, high-status occupation.
>
> The study reveals a high success rate for this program. One or two small incidents of a negative nature per forty-eight releasees should not cause the program to be dropped.

The report also included a section on computer crime. It read as follows:

> *Definition.* "Computer crime" is a broad topic that can be divided into several distinct categories. Many require little or no knowledge of data processing.
>
> The theft of trade secrets (programs, address lists, etc.), and the falsification of data prior to processing, are within the purview of persons with only a casual relationship to the data processing function. The misappropriation of computer time can be managed by computer operators, who may possess little knowledge of the internal workings of the machine. Also falling into this category are the malicious acts of destroying data and equipment by force.
>
> Crimes that require a highly-skilled and intelligence professional are: (1) The use of a computer to gain unauthorized information and, (2) The manipulation of programs or machines to embezzle. These are the only categories pertinent to this discussion.
>
> *Relationship to other white collar crime.* Using the computer to embezzle is the modern-day equivalent of "juggling the books." Programming involves the same kind of esoteric work assignment that makes it possible for accounting personnel to manipulate manual records to cover theft.
>
> Some methods employed are very similar to manual embezzlement. For example, "skimming," the practice of taking a few cents from many accounts and adding them to the account of the thief, is common to both automated and manual embezzlement.
>
> In other cases, the machine replaces a human collaborator needed to embezzle under manual systems. For example, bank programs have been altered to ignore the programmer's own account number when checking for overdrafts.
>
> Using a computer to gain access to unauthorized information is a form of espionage, closely akin to electronic surveil-

> lance. It differs primarily in that vaster quantities of information can be stolen with the same effort.
>
> *Scope of computer-related crime.* Current annual losses from all white collar crime are estimated at $40 billion. Losses from reported computer crime of all categories has been about $10 million per year for the past four years. Thus, computer related crime accounts for only 1/400th of losses due to white collar crime.
>
> There were 129 reported cases involving monetary losses from 1958 to September, 1975. The range of financial gain per case was $1,400 to $1.5 million; the average gain was $500,000 per case. Excluded from these figures is the loss from the Equity Funding case. The $2 billion embezzled in this single incident tends to distort the figures.
>
> While no crime can be completely eliminated in an open society, it is clear that the incidence of computer crimes can be reduced. One starts with the understanding that the opportunities for misuse are not unlike those for old-style embezzlement.
>
> In the Equity Funding scandal, in which computer programs were altered to fabricate over $2 billion worth of insurance policies, it was learned that the company's control was weak. There was no internal audit staff, and external audits were weak. The auditors never dealt directly with the computer staff.
>
> Programmers and analysts were permitted free access to computer operations; weekend work was permitted without supervision. Most of the hanky-panky, it was later revealed, occurred on weekends.
>
> It is evident from this and other incidents that the same kinds of common sense safeguards that thwart embezzlement under manual systems are indispensable for computerized systems. Separation of duties, dependable audits, and the use of cross checks are practices that should not be discarded when automation takes over the books.
>
> Prevention of unauthorized access through better hardware and software improves continually. GSA recently contracted with Stanford Research Institute to "crack" the security of the country's largest time-sharing vendor, Computer Sciences Corporation (Infonet). SRI was unable to do so.
>
> *Conclusion.* It is not necessary to restrain knowledge about computers to reduce computer crimes. It is more practical to apply common sense safeguards to computer systems; they are needed anyway to keep honest people honest.

Regarding the possible existence of refund fraud at the prison, Mr. Carlson's report mentions only the Frank Ready case. On this matter, the report states:

> Summary notes on matter of inmate Frank Edward Ready, #22178-175, committed to Leavenworth December 5, 1974, serving 5-year sentence out of Eastern Michigan for interstate transportation of forged securities.

During the time Ready has been serving in Leavenworth, two income tax returns were filed with IRS approximately one month apart. By accident both returns were reviewed by an examiner in IRS on the same day and the examiner noticed when looking at the second return that it listed a second head of household at the same address. The address in question was a residence on the outside and not Box 1000, Leavenworth. It turned out the second head of household for whom a $9,000 refund was claimed was Ready's 2-year old son.

At the time Ready was indicted for his attempted fraud by the U.S. Attorney in Kansas City, he was assigned to Leavenworth Camp. Upon his indictment, the institution moved him back inside. In gathering up his effects they found a letter he had written to his wife, several pages long, which described a number of fraudulent schemes, some involving IRS, being carried on by others in the institution. One such scheme described was in making multi-claims for IRS refunds with those claims being sent to different addresses, and the allegation that this scheme involved a total of $300,000 to $500,000.

Other allegations described schemes to defraud the Government with false G.I. Bill education claims. (This latter allegation paralleled the one recently investigated and found unfounded by the FBI.)

Ready is expected to go to trial on the income tax fraud next week.

Ready is not, and has not been connected in any way, with the computer/programmer training or production programs at Leavenworth.

THE McMILLAN MEMORANDUM

On June 28, 1976, committee staff met with Thomas V. Glynn, Assistant to IRS Commissioner Alexander; David Gaston, Director, Criminal Tax Division, IRS; Robert J. Potrykus, Regional Chief, IRS Intelligence, Dallas, Tex.; and Como Namorato, Chief, Criminal Section, Tax Division, Department of Justice.

At this meeting, the committee staff requested a copy of the nine-page memorandum prepared for Commissioner Alexander by the IRS Kansas City office. The staff had learned that this memorandum was written by IRS Intelligence Division Supervisor Robert McMillan of Kansas City. Also requested was a copy of the anonymous letter describing the alleged fraudulent tax refund scheme reportedly being perpetrated by inmates at Leavenworth.

In response to the requests on June 28, Thomas V. Glynn, on July 8, sent Senator Ribicoff edited versions of both the McMillan memorandum and the anonymous letter.

In a letter to Senator Ribicoff that accompanied the two documents, Glynn said that a work group of IRS officials had conferred and agreed on various proposals designed to detect and apprehend multiple filers. Seven of the proposals were implemented in 1976 and nine additional suggestions were under consideration during the 1977–78 filing period.

Glynn was then requested to keep the committee staff advised regarding developments in the Ready trial and also the progress of IRS Intelligence Division agents who were continuing their investigation of the allegations in the anonymous letters.

McMillan's memorandum traces the development of multiple filer schemes from prisons, gives the details of the allegations of additional fraudulent tax returns, identifies problem areas and gives conclusions and recommendations.

Regarding the *Ready* case, McMillan commented on how the fraudulent returns were discovered. He said:

> In March 1976, Internal Audit, while running a computer program to compare large refund returns, identified two returns with the same address, both of which claimed head of household status. An Internal Audit Trainee working under the direction of Internal Auditor, [deleted] identified these two returns on a computer printout where the names were side by side.
>
> In a discussion with [deleted] he stated it was his opinion that if the names had not been printed side by side, the fraudulent individual income tax returns of [the Readys] would not have been detected [deleted] stated that the returns merely would have been selected as a strong potential return for audit examination. Both of these returns, the first return filed in the name of [deleted] and the second return filed in the name of [deleted] claimed total refunds in excess of $18,000. The individual income tax return for 1975, bearing the name [deleted] showed a refund amount of $9,685.64 and had attached a W–2 form from the [deleted]. The U.S. Individual income tax return bearing the name [deleted] showed a refund in the amount of $9,797.89 and had attached a form W–2 from the [deleted]. The same day these returns were received by the Intelligence Division a telephonic Collateral Request was made to [deleted] and [deleted] to determine if the taxpayers had worked for either company during the year 1975. A negative reply was received. Each company had a former employee serving prison time in the Leavenworth Penitentiary. A computer printout verified that an inmate by the name of [deleted] was serving time in the [Leavenworth Penitentiary]. An inquiry at the two banks in [deleted] revealed that [deleted] wife of [deleted] had a bank account at the First National Bank where she had deposited refund checks.

Concerning additional allegations of more extensive fraud, McMillan wrote:

> An anonymous letter was received by the Internal Revenue Service on May 19, 1976, that had been mailed to the Federal District Judge [Edenfield] alleging that 600 fraudulent returns had been filed from the [Leavenworth Penitentiary] The anonymous letter states in general terms the facts and evidence obtained from the investigation of [Frank Ready]. The assumption had been made that the letter possibly could have been written by [Ready] himself. [Ready] would like

> very much to have charges against [Mrs. Ready] dropped when she in fact acted as an agent for him in cashing checks and transferring moneys and she herself actually filed fraudulent returns. This is not saying that the allegations alleged in the anonymous letter of more fraudulent returns being filed with the IRS is not possible.
>
> Tracing the funds fraudulently secured from tax refund checks through the bank accounts of [the Readys] did not reveal any additional funds other than the tax returns that we have identified as being fraudulent. Intelligence Division feels confident that we have obtained all of the fraudulent income tax returns filed by [Ready] from which he benefited. (In total [Ready], filed eight fraudulent income tax returns which generated in excess of $70,000 in fraudulent tax refunds during the years 1973 through March 1976) according to McMillan.

In discussing the identification of problem areas in the investigation, McMillan wrote:

> The investigation of [Frank Ready] disclosed that he knew enough about IRS procedures to discontinue using a social security number when a false return had been selected for an audit examination. A tax auditor in the [deleted] District had a fraudulent 1974 tax return of [Mrs. Ready] in her possession. Although the tax auditor had not been able to locate [Mrs. Ready] he was aware that the tax auditor was trying to examine one of the 1974 tax returns. [Ready] did not file a fraudulent return in 1975 under the social security number that was used on the 1974 tax return which was in the hands of the tax auditor for examination.
>
> It appears that the preparers of false income tax returns will use a fictitious name and a social security number that they know will not be used on any other tax return. In a search of [deleted] residence at [deleted] the agents found three newly acquired social security numbers that had been mailed to her from Chicago, Illinois, under the surname of [deleted]. It appears that the social security numbers probably belong to children who are not required to file income tax returns. Correspondence between [deleted] indicate that they knew they must acquire new social security numbers in order to avoid a duplicate filing situation.
>
> Information was obtained that [Ready] tried to secure 100 blank 1040 forms, in which [deleted] caseworker had refused to let him have inside the prison. Correspondence shows that [deleted] wrote his wife [deleted] asking her to smuggle three returns at a time into the prison until he had acquired 27 returns. In addition [deleted] provided him with employer tax guides, blank W-2 forms, and other publications the IRS provides to taxpayers.
>
> Refund checks were sent to addresses in which the occupants of the address never knew that a postman had delivered a refund check to their address. It is an assumption that [deleted] called the IRS office and inquired when his fraudulent refund would be released. Taxpayer Service

through IDRS would provide him with the date the refund check would be mailed if the fraudulent return had been posted. By this means [deleted] was able to send his wife or some other person to the residence where the check was to be mailed on or about the day such check was to be delivered. By taking the check out of the mailbox at the residence before the mail had been picked up by the occupant, there would be no trace of how or who acquired the refund check.

The rehabilitation program at the penitentiary provides a computer school in which they have 150 inmates enrolled. The director of the program stated that the inmates work night and day on various computer programs supplied to them through IBM and other computer companies. The prison has the capabilities and facilities to actually program our DIF scores and create a model tax return that would be readily accepted when filed with an Internal Revenue Service Center. Analysis of cases where Intelligence has found fraudulent returns within the prison show that each time there is a conviction, they have tried to eliminate the flaw in their fraudulent return scheme. Examples are as shown below:

1. In the early 1960's, fraudulent returns were mailed from the prison, now the returns are mailed from outside the prison.
2. Originally refunds would come to the jail or to a post office box, now no two refund checks will go to the same address.
3. It is evident that inmates know they must have good social security numbers and good employer identification numbers on their W-2 in order to beat the system.
4. After Frank and Melinda Ready are tried, it is probable that inmates will use fictitious names instead of aliases.
5. Inmates receiving the refunds or whose family will receive the refunds make sure that their handwriting is not on the fraudulent return. [Deleted] stated, after he was convicted, that the only mistake he had made was in actually signing the return himself.
6. The fraudulent tax return claims for refunds have risen from $600 per refund to $10,000 per refund.

As you can see, through the years the preparers of these fraudulent returns have improved their scheme. An analysis of the known fraudulent claims that were generated by inmates within the Region shows the alarming fact that each one of these cases originated from leads uncovered by accident, an informant, or by prison guards who noticed inmates receiving more than one income tax refund check. It is also an alarming fact that inmates, who have been exposed to the fraudulent income tax scheme, have taken their knowledge to the outside of the prison when they have been paroled or otherwise released.

It is obvious that the IRS can only eliminate this problem of false individual income tax returns claiming fraudulent refunds by matching the 1099 and W-2 forms with individual tax returns. The whole scheme is predicated upon the widely known fact that such a matching process does not exist within the IRS other than on a limited scale.

The next best solution would be to go back to the prior refund audit program. This would entail making a selection of returns that claim refunds and have them audited before the refunds are released to the taxpayer. This is not very acceptable because it will delay honest taxpayers from getting their legitimate refund checks within the prescribed time that the IRS has promised such checks.

Internal Audit within the Service Centers has in the past instituted various compliance checks in the form of computer programs to identify large refunds being issued to taxpayers. As Internal Auditor [deleted] has stated, it was only by accident that the two [Ready] names were printed out side by side to detect the fraudulent returns. Although this program would be beneficial, it certainly was not designed to detect 600 returns that could have been filed at the Leavenworth Prison in 1975.

Another suggestion was made that the social security numbers and names of all Federal penitentiary inmates be programmed to match up any returns that may have been filed. Such a program could be instituted, but it would be ineffective if other social security numbers are used along with fictitious names.

Until the Intelligence Division develops computer capabilities within the Service Centers to detect fraudulent refunds and other Title 26 violations, the IRS will be left with the tools of detection we are now using such as informants, close liaision with officers of the Federal prisons, and detection by chance or accident.

In the [deleted] case it was suggested to the National Office that a program be created to extract returns that had the same dollar amount of refund that the inmates were known to have received. It was decided that this program would be ineffective in that some of the refunds were issued in different amounts.

It should also be noted that in the [deleted] case the fraudulent returns that he filed in the years 1973 through 1976, involved four regions and four different Service Centers. Any computer program would have to be used in all Service Centers to get the coverage needed to detect these fraudulent returns. Programs, which the Service Centers have created, identifying refunds going to the same address detects refund mills but would not detect the fraudulent returns such as those being filed by inmates in the Federal prisons. The scheme appears to be spreading outside of the prison walls.

[Deleted] District has two individuals under investigation who fraudulently received a $23,000 refund. The [deleted] District has information that some 300 tax returns were to be filed by a church and there is no way of determining if such returns have been filed.

> Another consideration that could be considered is using a tax number rather than a social security number that an individual would file under each year until his death. This would help the Internal Revenue Service track tax returns that have not been filed, but it too is not practical and is probably a violation of an individual's rights.
>
> I do not believe at the present time the IRS has sufficient capabilities to detect the fraudulent tax returns being filed by the convicts. I do believe we have made progress in shortening the investigation time by using Title 18, Section 641 under the direction of the U.S. Attorney. I would recommend that the Intelligence Division be given the authority to use Section 641 on a limited basis or that the Service recommend a similar statute to be added to Title 26 of the Internal Revenue Code.

The Ready trial, originally scheduled for June of 1976, was postponed. Ready remained in prison.

McMILLAN IS INTERVIEWED

IRS agent Robert McMillan was interviewed in Washington by Committee Investigators on August 5, 1976. McMillan was accompanied at the interview by Donald Turley of the Washington office of the IRS Intelligence Division.

McMillan said that because the *Ready* case had not been brought to trial yet he was limited in what he could tell the committee. McMillan also qualified to some extent one aspect of his memorandum of June 11, 1976, to Commissioner Alexander. In his memorandum, parts of which have already been printed in this staff study, McMillan referred to the ability of the prisoners at Leavenworth to "Actually program our DIF scores and create a model tax return that would readily be accepted when filed with an Internal Revenue Service Center."

McMillan said that this opinion of his may have been premature and that, in any event, he did not mean that the possible capability of the inmates to program DIF scores necessarily had anything to do with the computer training and rehabilitation project at Leavenworth. DIF stands for discriminate function and, according to the Library of Congress, is a "Process that cross checks as many as 15 to 20 items on a return, assigning numerical weights to return characteristics and identifying returns with a high probability of error. Returns with high DIF scores are channeled to groups of IRS examiners who look over the returns to combine computer scoring with human judgment to arrive at a decision to audit or not."

This definition comes from the Library's Congressional Research Service, Economics Division, and appears in a CRS Multility, No. 76-68E, entitled "Internal Revenue Service: History and Matters Dealing With Oversight Of Its Practices and Procedures Through 1974."

McMillan said that convicts could learn about IRS computer tolerance levels by trial and error, by reading readily available material on tax preparation and by access to IRS information recently released under Freedom of Information requests. He said that he had no tangible proof that the computer operation at Leavenworth was involved in any fraudulent scheme aimed at IRS refunds.

McMillan said that after the trial of Frank Ready more information may become available regarding the possible participation of other inmates in schemes. These inmates may have had connection with the computer operation, McMillan said.

McMillan said that although his investigation was incomplete, IRS had been able to verify some of the information in the anonymous letter.

McMillan identified Louis McGill of the Internal Audit Division in Dallas as the supervisor whose unit had uncovered the *Ready* case from computer printouts.

MEETING IS HELD AT GSA

On Wednesday, August 11, 1976, committee staff attended a meeting at the General Services Administration to discuss issues pertinent to the overall computer inquiry including questions concerning personnel security and GSA regulations requiring Federal agencies to clear through Federal Prisons Industries for ADP services.

The meeting was held in the office of Theodore D. Puckorius, Commissioner of GSA's Automated Data and Telecommunications Service (ADTS). Puckorius attended as did Nancy Doane of Puckorius's staff; Robert Seraphin, Chief of the ADTS Technical Branch; Michael Munter, Acting Assistant Commissioner for Planning and Policy; and Betty Karabatsos and Gayle Chrzan, both of the GSA Office of Congressional Affairs.

Puckorius said security considerations in the ADP field were not the responsibility of GSA.

Puckorius said he did not know what personnel security standards were applicable to the use of convicts at Leavenworth in programing ongoing Federal ADP projects such as the Department of Agriculture's Agricultural Stabilization and Conservation Service (ASCS).

Puckorius said he did not know whether the convicts employed by FPI programing services at Leavenworth were Government employees or Government contractor employees or, more precisely, just what status of employee the inmates enjoyed. He said he did not know whether the inmate programers were eligible for Federal employment in the ADP field after their release from prison. Puckorius said that to his knowledge these issues had never come up, that he had neither sought nor received any direction from the Office of Management and Budget (OMB) or the Civil Service Commission on these issues. Puckorius said he would direct his staff to look into issues concerning personnel security in connection with the Leavenworth prison situation and also in connection with commercial firms which provide ADP services for Federal agencies.

Puckorius said he agreed with an assertion by the committee staff that there is a certain inconsistency in a Federal policy that allows felons in prison to program Government computer projects but may find the felons unqualified for Government employment in similar projects when they are released from prison.

OMB POSITION

On August 25, 1976, Walter W. Haase, Deputy Associate Director for Information System of the Office of Management and Budget, was interviewed by committee staff. When asked whether convicted felons could obtain Federal employment in the ADP field, Haase replied that: (1) he did not know what procedures were required or followed to preclude such employment; (2) to his knowledge there were no hard and fast rules on this subject matter; (3) it was his belief that a felony conviction would not necessarily disbar a person from being hired as a computer programmer; and (4) aside from issuing regulations which affect the pertinent provisions of the Privacy Act of 1974, he was unaware of any requirements and criteria promulgated by Civil Service Commission on personnel security in the ADP area; the subject had not been previously discussed per se, he said.

USDA OFFICIALS DISCUSS PROGRAM

On August 26, 1976, committee staff met with Robert Head, Assistant Director, Automated Data Systems, Department of Agriculture, and James Dinwiddie, Director of USDA's Data Systems Division, Agricultural Stabilization and Conservation Service (ASCS).

Dinwiddie confirmed that the programs written by inmates affect the accounting and general ledger programs of ASCS and, therefore, do affect the disbursement of funds for various agriculture support, loan, and conservation programs.

Dinwiddie said that several programs written by inmates do affect Internal Revenue Service records in that ASCS computers report to IRS all amounts of reportable payments to individuals who receive agricultural funds. This programing work is conducted under the title of "Producer Payment Reporting System."

Dinwiddie and Head said that they did not know what personnel security standards or selection standards, if any, were used to designate inmate programers but, they said, certain inmate programers at Leavenworth would probably not be eligible for Federal employment in similar positions with the Agriculture Department.

Dinwiddie, however, was generally supportive of the Department of Agriculture's use of FPI computer services and said that he was unaware of any abuses in the program or any fraud connected with it.

As a result of the meeting with Head and Dinwiddie, a written response from the Agriculture Department was sent to Senator Ribicoff. Dated September 21, 1976, the letter was signed by J. Paul Bolduc, Assistant Secretary for Administration. In that portion of his letter which dealt with the relationship of ASCS to the FPI/Leavenworth inmate programers, Bolduc said:

> . . . The original interagency agreement between the Agricultural Stabilization and Conservation Service (ASCS) and Federal Prison Industries, Inc. (FPI), was signed August 7, 1972. Since that time, it has been amended twice. These documents, together with the annual financial agreements, describe the scope, terms and conditions under which ASCS obtains programming services from FPI.
>
> Selection of inmate participants in the program is handled exclusively by Bureau of Prisons/FPI personnel. ASCS has reviewed the screening process and does not impose any additional requirements.

> Programs that are written by FPI personnel are subject to the following processes prior to being placed in production.
>
> 1. The programs are checked for COBOL assembly errors.
> 2. For approximately 50 percent of the programs a flowchart is prepared using Autoflow.
> 3. Source program and/or flowchart is reviewed to assure program satisfies the requirements as specified in the program/system specification.
> 4. For all programs the unit test data and test output product provided by FPI are reviewed for completeness and accuracy.
> 5. The next step is to compile and link the program to the appropriate system section's test executable library (source program has already been placed on section's test source library by FPI coordinator) and to prepare the Job Control Language required for use in integration testing.
> 6. All programs are subjected to a complete integration testing and review of the output product by system section personnel.
> 7. Programs are subjected to an acceptance test and the output products of the system are reviewed by additional personnel to insure the ouput product is accurate and complete.
> 8. Only when all of the above actions have been accomplished is a program placed into production.
>
> The Performance Monitor of METACOBOL is being used for programs developed by FPI as well as in-house products. Even though the purpose of this monitor is primarily to provide information relative to the efficiency of program design and compiler generated code, a part of this output specifically identifies "unexecuted" paragraphs. This "Paragraph Table" is a list of paragraphs known to the performance monitor and reflects "wait-time" and "active-time" distribution percentages as well as paragraph execution counts.
>
> These checks are standard procedure for program development. No additional checks are performed for FPI generated programs.
>
> . . . A search of the Master Name and Address File maintained on magnetic tape in Kansas City and the records, including address plates in the Leavenworth ASCS County Office has revealed no indication of any mailings to Box 1000, Leavenworth, Kansas [the prison mailing address].
>
> The USDA Office of Investigation has no present or past activities related to the U.S. Penitentiary at Leavenworth.

With his letter, Bolduc submitted five attachments. The attachments describe the services which are provided by the computer programs written by the Leavenworth prisoner programers. Information contained in these attachments indicates that the Leavenworth inmates write the computer programs which have facilitated and controlled the distribution of billions of dollars of public funds disbursed by the Agriculture Department in support of various conservation, disaster relief and loan programs.

Bolduc cited 17 ADP applications programed by Leavenworth inmates. Here is how Bolduc described the applications:

1. *Commodity loans and purchases*

   Records individual loan and purchase data for all eligible commodities. Loan activity includes loans made, repayments and forfeitures for both farm and warehouse stored loans. Financial and statistical reports are made from loan summary files.

2. *Loan Certification*

   Records, verifies and reports on inspections and measurements made by county office personnel on selected producer certified farm stored loans.

3. *Farm Storage and Drying Equipment Loans*

   Records data on farm storage and drying equipment loan including disbursements, repayments and account status. Prepares required management reports.

4. *Producer Payments Reporting*

   Records producer payments for summarization and annual reporting to IRS and the producers. A producer name and address file is maintained for use with this system and other systems as well. Approximately 760,000 statements were prepared and mailed to producers on payments received in calendar year 1975.

5. *Disaster program payments*

   Records payments made, checks compliance with payment limitation provisions and provides progress reports to management on feedgrain, wheat, cotton and rice.

6. *Wool and mohair program*

   Processes applications for payment, computes payments due and prepares sight drafts for verification, signature and issuance by county offices. Prepares reports on program accomplishments.

7. *Tobacco program*

   Maintains data on burley and flue-cured tobacco farms, producers and warehousemen/dealers including sales and purchases. Produces allotment and quota notices, marketing cards and program reports.

8. *Processed commodities inventory*

   Assists in the inventory management activities for processed commodities including their acquisition, storage, transportation, handling and disposal along with related payment operations.

9. Grain inventory

Assists in the inventory management activities for CCS owned grain including acquisition, storage, reconcentration, transportation, sale, donation and settlement operations.

10. Sight Draft Accounting

Maintains a complete draft issued file on all CCS sight drafts for reconciliation with paid data received from FRB. Disbursement data is transferred to various other computer systems for use in the preparation of program reports.

11. Appropriated Fund Accounting

Assists in accounting and reporting activities for ASCS appropriated funds including allocation, limitation, cost distribution, fund distribution and other related data.

12. County Office Administrative Expense

Records and maintains data on funds allocations, sight draft limitations and county office bank accounts along with personnel and payroll information for each county office employee and county and community committeemen.

13. County Office Work Measurement and Fund Allocation

County office workload is measured on a sample basis for analyzing each major program activity in the sample counties analyzing each major program activity in the sample counties. Fund allocations are made to all county offices based on regression coefficients developed in the sample work measurement activity.

14. Conservation Reporting System

Provides for the entry and accumulation of individual producer performance data for Agricultural Conservation Program (ACP), Emergency Conservation Measures (ECM), and Naval Stores Conservation Program (NSCP). The data is supplied to the accounting and producer payments systems as well as being used for periodic progress and statistical reporting purposes. Program payment limitation provisions are checked for compliance. A similar system is maintained on the Forestry Incentives Program (FIP).

15. Accounting, Budgeting and Reporting System

Supports both ASCS and CCC fiscal accounting. Separate general ledger controls are maintained for ASCS and CCC funds. Produces specified fiscal reports including accounts analyses, reports of financial conditions and fiscal operating reports.

16. General Sales Manager Export Program System

Supports accounting and reporting for CCC export programs including credit sales and PL–480 programs.

17. Miscellaneous Systems

Several small administrative-type systems are maintained to support ACSS activity such as CCC Budget-Supply and

Utilization, Defense Facility Listings, Administrative Property Records and Work Measurement Reporting, and a Ground Truth Data System for the Large Area Crop Inventory Experiment (LACIE).

Documentation provided the committee by Bolduc describes the actual programs written by Leavenworth inmates from 1972 to 1976. This documentation shows the extent to which the programs written by prisoners affect other computer operations. Directly or indirectly, the programs cited by Bolduc as having been written by prisoners result in the disbursement of Government money. Here are some examples provided by Bolduc of programs which have been used at the Agriculture Department's Kansas City Computer Center and which were written by prisoners at Leavenworth:

1. Financial and Budget Master ASCS Balance Exceptions—D331520F

The Update and General Ledger segment of the Financial and Budget Master System, of which this module is a part, uses current accounting transactions to update the Financial and Budget Master file. Various updating, closing, purging, balancing and reporting functions are included. This module uses specified exception formulas to determine if ASCS or OGSM data is in an out-of-balance condition. All formulas are printed. Formulas with an out-of-balance condition are flagged.

2. CCC Fiscal Reporting Income and Expense—D34111OAD

This modular program is called by the handler program whenever there is a request for the Comparative Statement of Income and Expense report. This run accesses accounting data on the Financial and Budget Master file, line title data on the CCC Fiscal Reports Stub file and prior year data on the Prior Year Financial file. It compiles all this information into a report format for inclusion in the "Report of Financial Condition and Operations" booklet.

3. ASCS Allotment and Cost Distribution Correction Process Control Module—D355150

This program will serve as the controller to call modules to effect the correction activity processing along with modules pertaining to allotments and cost records. This program controls the calling of program modules to accomplish the correction processing, controls, allotment, transportation, cost distribution, and cost recap proof listings.

4. Total Amount Shipped Report—F444460

The purpose of this program is to produce a report reflecting shipments of commodities under PL480 Title I, and the countries that those shipments were made to the report is produced twice a year and accesses the Bill of Lading data base and the reference files for Country and Commodity information. The data is grouped into six months periods for the last three years and then lumped together from that point back to the beginning of the PL480 Program.

Data reported is:
Type of Sale,
Market Value,
Quantity (usually metric ton).
These are by commodity with a total of each country.

5. *Loan Excise Tax Register Produce Proof Listing of Adjustments to Excise Tax Register A1172280*

The purpose of this program is to validate, sort and prepare a prooflisting of cards for excise tax withheld adjustment items for commodities; wheat, flax, peanuts, rice and soybeans. These adjustments are for any loans reported on the monthly Excise Tax Register for which it is determined an adjustment must be made. The following validities are performed: state code must be valid, county code, loan number, transaction code, crop year, transmittal number, disbursement date, quantity and tax must be numeric. Commodity code and loan type must be valid.

6. *Farm Storage Facilities (FSF) System Overview*

Loans made under Farm Storage and Drying Equipment Loan Program help finance grain storage structures and equipment used by producers to store and care for grain on farms.

The major portion of the transactions in (FSF) system are loans made and loans repaid. Loan disbursements are made by CCC sight draft and data is received from the Draft Accounting System (DRAC). Loan repayments (CCC-257) are initially recorded in the Cash Receipts Segment of the Financial Accounting System (FAS).

Repayments in the form of setoffs against the proceeds of a commodity loan are received from the Price Support Computer System. Thus, the bulk of the transactions are received from other computer systems. The remaining transactions, claims and corrections are entered by punched cards from source documents received from county offices.

Transactions are validity checked and accounting outputs and operating reports are produced either in lists or magnetic tape. Reports are produced monthly, quarterly, semiannually and annually. A report data tape is produced for the OEO Computer System.

7. *Farm Storage Facility and Drying Equipment Loans System (FSF) Sort Accepted Data—A185020*

This program sorts accepted FSF data into State, County, Loan Number, Program Code, Transaction Code and Accounting Date sequence.

8. *Farm Storage Facility and Drying Equipment Loans System (FSF) Prepare FSF State and County Reports—S185050*

After the update of the FSF loan file with monthly activity, the file is processed to produce the following:

A. A tape of loans and disbursements made during the month for OEO reporting.

B. Small balance records for those loans having a principal outstanding of $3.00 or less.
C. State reports for all loans.
D. National report for all loans.
E. Small balance print list.

This program is run monthly at month-end.

9. Farm Storage Facility and Drying Equipment Loans System (FSF) Prepare History Microfilm List—A185088

The purpose of this program is to list annually all FSF Loan Transactions followed by the Loan Summary record. This history list is used to reconcile the CCC 386 Report for FSF Loans. This run creates print tapes and a microfilm tape.

10. Financial and Budget Master Overview

Journal voucher input data is received from DSFO, PVCO, FI, and other DSFO computer systems (i.e., Financial Accounting and Appropriated Fund Program Accounting Systems). All input data is validity checked and balanced, and listings are produced, by office, for control and research purposes.

Rejected journal voucher data is retained on suspense file to facilitate correction processing. Accepted journal voucher data files are subsequently processed to:

Produce general journal listings, by office,
Produce inventory costing reports for DSFO and PVCO,
Update the master file.

The master file is used to produce the general ledger and trial balance listings, by office, and for all offices combined. The master file is also used to produce fiscal reports.

All the system listings are produced separately for each agency (i.e., ASCS, OGSM, and CCC).

11. Financial and Budget Master Check, Sort and Format Input—D331120

New Journal Vouchers and/or correction vouchers from Washington, D.C., Kansas City, Minneapolis and the Financial Accounting System, as well as Contra Vouchers from previous processes of this system are subjected to several pre-validation checks, encoded in this program, necessary to format the output records. The input information is rearranged into a common format and sequence compatible to further AB&R processing. Finally, the two types of records corrections and new vouchers, are written to two separate disks to allow their processing by two subsequent programs with separate functions.

12. Financial and Budget Master General Ledger Title Creation—D331527

Key-punched General Ledger line item titles are processed in this program, to produce initially, or change an existing tape file which, in turn, is used to control the printing of the General Ledger Report. After creation or changing the

General Ledger Titles File, the file is printed. An Exception Report is printed during the processing of this program to list discrepancies, changes, deletions and additions as they occur.

13. Fiscal Reporting System Overview

This system builds reports regarding the financial condition of the Commodity Credit Corporation and of the ASCS appropriations. These reports are as follows:

1. Comparative Balance Sheet.
2. Accounts Receivable and Payable.
3. Income and Expense.
4. Interest.
5. Donation of Commodities.
6. Disposition of Inventory.
7. Net Gain or Loss on Inventory.
8. Investment in Loans and Inventory.
9. Statement of Financial Condition for Treasury.
10. Analysis of Appropriated Funds.
11. SF133 Report on Budget Execution.

14. CCC Fiscal Reporting Accounts Payable, Accrued Liabilities, Trust and Deposit—D341110AC

This modular program is called by the handler program whenever there is a request for the Accounts Payable, Accrued Liabilities, Trust and Deposit Liabilities and Other Liabilities reports. This run accesses accounting data on the Financial and Budget Master file and formats this data for inclusion in the "Report of Financial Condition and Operations" booklet.

15. Fund Distribution System Overview

The system summarizes, records and builds reports for cash transactions processed through the Federal Reserve Banks, regional disbursing offices and Treasury. It provides card data for Treasury to record certificates of deposit. Detail is provided on reports for manual preparation of the SF224 (Statement of Transactions).

16. Fund Distribution System Program D354300—Monthly Process Control Program

The purpose of this program is to control the execution of the programs that are required to perform the monthly processing. Based upon codes returned by the called programs this program will call or bypass other programs. It also produces a report that shows the activity that has occurred.

17. ASCS Allotment and Cost Distribution Daily Activity Control Module—D355100

This program will serve as the controller to call modules to effect the Daily Activity Processing of the Allotment and Cost Distribution System. This program controls the calling of program modules to accomplish the daily input, control, trial balances and preparation of proof listings.

18. Non-Producer Payments Reporting System Overview

Master Name and Address and Index Table files of non-producers with the potential of receiving CCC payments have been established. Payee identification codes for all known potential payees are included in the Index Table file. An office code prefix is utilized to eliminate possible duplicates between offices. In addition, a unique code is assigned to each parent and independent (unaffiliated) company. A single name and address for each unique code is maintained on the Master Name and Address file. The Index Table file relates all payee identification codes (for parent, independent and submisiary companies) to their respective unique codes, allowing subsequent summarization of payee data. Both files are updated monthly upon submission of payee data.

Payment data is received for disbursements made to non-producers by Fiscal Division (FI) and the Prairie Village Commodity Office (PVC). Each payment record includes a purpose of payment code and payee identification to allow summarization for reporting purposes. FI Division payment data is furnished on source documents for key punching at DSFO. PVCO manual draft data and computer prepared draft data is selected from the Sight Draft Accounting System and the Financial Accounting System. PVCO collection data is punched on cards.

All payment data is processed by the end of the month in which received. Control and rejection listings are furnished to Data Operations Section (DOS) for distribution to the appropriate office. Corrections are submitted with subsequent month data.

Reporting is processed on a request basis. Normally reports are requested at the end of a fiscal year for that year's payments.

19. Non-Producer Payments Validity Check—D366064

This program is designed to validity check the non-producer payment data records that are submitted by the Commodity Offices and the Fiscal Division in Washington, D.C. These payment records come from three different sources. Payments that have been mechanically prepared come from the financial Accounting System. Manually prepared payments from the Commodity Offices come from the Sight Draft Accounting System. Payments from the Fiscal Division are key-punched and entered via punched cards. Valid payment data records are passed on to the monthly update process. Invalid payment data records are formatted and printed to be returned to the respective submitting office for correction and re-entry.

20. *Non-Producer Payments Select and Accumulate for Reporting—D366108*

This program is designed to accumulate all Master Payment Data File records with the same Unique Address Code. These accumulations are also by purpose of payment.

After these accumulations are made, they then must be matched to the Master Address File to obtain the nonproducers name and address. This program is run on request of the Administrator, Agriculture Stabilization and Conservation Service. This request may also be for optional data (producers receiving over a million dollars, producers receiving less than a million dollars, all producers, the 50 producers receiving the highest amount of payments, etc.). This request may also be for optional sequences (alphabetic, amount in ascending sequence, amount in descending sequence, etc.).

21. The following programs sent to FPI have not been placed in production but are currently in acceptance test stage

F452120—FIP Sight Draft Validation
F452130—IRS Initial Update
F452200—Combine Sight Draft and FIP–13 Date
F452140—Combine Sight Drafts
F452220—Update FIP File
F452230—Prepare General Ledger Entries
F452240—Prepare Budget Report
F452280—Prepare Allocation Control
F452300—Prepare Research List
F452340—Prepare Statistical Report Date

THE TRIAL OF FRANK READY

On August 31, 1976, in a Federal court in Kansas City, Kans., Frank E. Ready, 31, a convict at the U.S. prison in Leavenworth, went on trial for tax fraud. Ready was charged with having filed false tax returns that resulted in his receiving more than $20,000 in refunds for 1975.

The trial ended on September 9, 1976. Ready was convicted and sentenced to 15 years. Since Ready was already incarcerated, the sentence was to run concurrently with his present term, 5 years for interstate transportation of stolen securities.

Ready's former wife, Melinda, was also charged and convicted in connection with the tax fraud. Melinda received a 6-month sentence and 3 years of probation.

As has been indicated earlier in this staff study, Frank Ready was not at the time of his arrest, nor had he ever been, a participant in the computer training and rehabilitation program at the Leavenworth facility. However, as part of his defense during his trial, Ready sought to show that he had been framed by other inmates at Leavenworth.

One of the inmates Ready named was Sherrold Gaston (Skip) McLain. Skip McLain was a participant in the computer training program at Leavenworth. Ready alleged, in fact, that Skip McLain was a mastermind in a conspiracy at Leavenworth to compromise IRS computers and, thereby, initiate actions resulting in many tax refunds being sent to McLain and his accomplices.

Independent inquiry by the committee staff indicated that Sherrold Gaston (Skip) McLain was enrolled in the computer program at Leavenworth from September of 1975 to January of 1976. In January of 1976, agents of the Federal Bureau of Investigation made inquiry into allegations that McLain was involved in GI Bill fraud and loan sharking in the prison. Prison authorities removed McLain from the ADP project and placed him in isolated confinement. No charges against McLain resulted from the FBI investigation. Later in January of 1976, McLain was transferred to the U.S. Penitentiary, Atlanta.

Ready was unsuccessful, for the most part, in his effort to introduce evidence during his trial to demonstrate that other prisoners had set him up. Much of the evidence and testimony which Ready's defense attorney, Thomas Dawson, wished to use in the trial was not allowed on evidentiary grounds. The court ruled that such evidence was not pertinent or was inadmissible hearsay or was irrelevant to matters referred to in the original indictment.

Defense attorney Thomas Dawson spoke with news reporters at the start of the trial. Dawson was quoted as having said Frank Ready was the victim of a frameup and that other inmates associated with the computer school were to blame. Neither Dawson nor Ready, however, was the source of information developed by the committee staff in May of 1976 in which it was alleged that a group of convicts at Leavenworth had figured out how to "beat" IRS computers, were filing fictitious returns and were receiving tax refunds.

The Kansas City Star of September 3, 1976 quoted Dawson as saying, "Our evidence will show that a number of inmates [at Leavenworth] developed through the use of the computer a way to file tax returns that they thought would pass through the Internal Revenue system without audit." However, no conclusive evidence in support of Dawson's assertion was ever presented during the trial.

Defense attorney Dawson did succeed in presenting testimony aimed at demonstrating that Skip McLain was involved in a scheme to defraud IRS and that McLain had in his possession documents which implicated him in such a scheme. Dawson elicited this testimony from two inmates at Leavenworth—Paul Joseph Mosier and Alfred Hill Lisk.

Mosier, like Skip McLain, had been a participant in the computer training program at Leavenworth. Responding to questions from defense attorney Dawson, Mosier testified at the trial that he began his current sentence at Leavenworth in December of 1974. Mosier said he was found to have tuberculosis and was quarantined in the prison infirmary. Because he had been employed in 1974 prior to his incarceration, Mosier was obliged to file tax returns for 1974 with IRS from prison, Mosier said. But, Mosier testified, he did not know how to file. A prison counselor recommended that he seek the help of Frank Ready, Mosier said, explaining that Ready was working as a clerk in the infirmary at the time.

Convict Mosier testified that convict Ready helped him fill out his tax returns. Mosier said his returns noted the fact that he had been employed in 1974 by the Tomack Construction Company of Oklahoma City and National Management Services, Inc., of San Angelo, Texas.

Mosier testified that he met Skip McLain while he and McLain were enrolled in the computer training program at the prison.

Mosier testified:

> I'm in the computer school at the penitentiary and Skip McLain was also in the school. We became acquainted. On weekends we started getting together playing cards and

> things and one day he told me that he had a tax scheme that we could make a lot of money off of but you needed some people on the streets to have checks sent to and wanted to know if he could send my fiancee some checks or have some checks sent to her. I wasn't interested at all because I didn't want to get my girlfriend involved in it at all so I told him I didn't want to have anything to do with it.

Questioned further by defense attorney Dawson, Paul Joseph Mosier testified that Skip McLain did not describe his tax scheme in any detail. Mosier said McLain was aware of the possibility that his scheme might be uncovered. But, Mosier said, in the event of detection, McLain felt he could arrange for another Leavenworth convict to be blamed. "When I expressed concern about" getting caught, Mosier testified, McLain "told me that if any heat came down there was someone out at the camp that he could shift the heat to." Inmates about to be released or considered to be appropriately trustworthy are assigned to a camp outside the Leavenworth prison walls.

Mosier said the conversation about the tax scheme had taken place with McLain in the fall of 1975. Mosier said he had no further dealings with Frank Ready after his illness cleared up and he was released from the prison infirmary. However, since they had become friends at the computer school, Mosier and Skip McLain continued to be friendly and see each other regularly until McLain was removed from the prison population and confined in isolation. Mosier and McLain were friendly enough with each other to exchange combination locks for lockers they had to safeguard personal belongings.

Mosier explained:

> One day Mr. McLain came to me and told me someone had known the combination of his lock and was getting into his locker and asked me if I would trade locks with him. We have combination locks at the penitentiary. We traded locks, figuring that no one would know we had traded so they wouldn't know his combination and wouldn't know what he had done with the lock he had, so I ended up with his lock and he ended up with mine.

Unfortunately, Mosier may have fallen prey to the old switching locks trick. Mosier testified that now that Skip McLain's lock was on his locker he began to notice that things were disappearing from the locker. Among the personal papers which were missing, Mosier said, were his tax information sent to him by his two previous employers in 1974, the Tomack Construction Co., and National Management Services, Inc., as well as other documents he had used in filling out his tax returns for 1974.

Exhibit W at the Ready trial was a sheaf of binder paper with typewritten notations. Exhibit W was obtained by the committee staff from the trial records. Exhibit W, according to an evaluation by the committee staff, appears to be a step-by-step set of instructions on how to compose fraudulent tax returns for the purpose of receiving a tax refund. Exhibit W includes instructions detailing how would-be tax law violators can obtain another person's social security number, business tax identification number and W-2 forms.

For example, a proposed scenario spelled out in exhibit W says that one method of obtaining another person's social security number is to run an advertisement in the newspaper saying a business is looking for youngsters for employment. A telephone number is indicated and interested youths are urged to call. Then, when a teenager calls, the would-be violator asks for the youngster's name, address, social security number, and telephone number and promises to call back. The youth, enthusiastic about the prospect of a job, gladly obliges. The would-be violator does not return the call. But he now has the youngster's legitimate social security number. A genuine social security number significantly enhances the opportunity for a violator to file a fictitious tax return that will result in an IRS refund being sent to him, independent inquiry by the committee staff revealed.

Exhibit W also spells out various formulas and equations indicating when refunds will be returned from the date of filing. Independent inquiry by the committee staff indicated that a violator filing a bogus tax return would have several reasons to want to know when the refund was likely to be mailed back. For example, if the violator used the name and address of an innocent person, the violator or an accomplice could intercept the refund check—perhaps by stealing it from the innocent person's mail box—if he knew precisely what day the check was likely to arrive.

Exhibit W—the sheaf of paper—was found in the Leavenworth prison among the personal belongings of Frank Ready.

Leavenworth convict Alfred Hill Lisk was asked at the Ready trial if he ever saw exhibit W while in prison. Lisk said he had seen the sheaf of paper, or something very similar in appearance to it, in the possession of Skip McLain.

Lisk was not enrolled in the computer training program at Leavenworth. Lisk said he knew both Frank Ready and Skip McLain from prison. Lisk said it was he, in fact, who introduced McLain to Ready.

Responding to questions from Ready defense lawyer Thomas Dawson, Alfred Hill Lisk testified that he had never heard McLain talk about a scheme to perpetrate a fraud on IRS. But Lisk did say that McLain came to him one day and asked to be introduced to Frank Ready. Lisk said Frank Ready was well known in the prison for being able to help people with their tax returns. Prisoners, as well as prison guards, came to Ready for tax preparation assistance and Ready accommodated them, Lisk said.

Lisk testified that once he had introduced Skip McLain to Frank Ready the two new acquaintances—Ready and McLain—immediately began discussing taxes and how to file returns. "I did introduce him [McLain to Ready] and they talked about tax matters," Lisk said, adding that "They had several forms laying out on the table."

Shown the sheets of paper that made up exhibit W, Lisk testified that he had seen the documents, or similar looking papers, in McLain's possession.

> This [exhibit W] is in a box underneath his [McLain's] bed in his cell. He and I lived—our cells were right close and we had access to each other's cells. We shared a number of things. This was in a box . . . I asked him about this one time because it is obviously some kind of sham and I don't remember what he answered me.

Exhibit 92 was introduced at the trial. Exhibit 92 is a notebook containing handwritten information on check drops, dates for mailing returns and receiving refunds, projected returns totaling several million dollars and other writings in code and abbreviation indicating that certain persons in various cities throughout the Nation were to receive tax refund checks.

Exhibit 92 was found among Frank Ready's personal possessions in prison.

Alfred Hill Lisk was asked at the trial if he had ever seen exhibit 92, the notebook. Lisk replied:

> Well, I can't—Skip had a book like this. Whether this is his book or not, I don't know. I don't recognize any of the——

Defense attorney Dawson interrupted Lisk at this point to ask if Lisk's meaning was that he, Lisk, had seen Skip McLain with a notebook that looked like exhibit 92 but "you can't recall specifically."

"Very similar to this," Lisk testified. "He had one which is unusual out there because most guys don't have access to books like these. Whether this is his book or not, I don't know."

Convict Lisk could not positively identify exhibit 92. Similarly, convict Paul Joseph Mosier said of exhibit 92: "I can't be positive it is the same. But I've seen one like it, if it's not this one, in Mr. McLain's possession."

The committee staff obtained a copy of exhibit 92 from the court records.

During the Ready trial, defense attorney Thomas Dawson did attempt to have Skip McLain and two other convicts who had served in Leavenworth—Donald Allan Walters and Emmitt Jefford—called as witnesses. In his motion to have McLain, Walters, and Jefford testify, Dawson contended that Ready was framed to cover up for the guilt of other prisoners who had tried to perpetrate tax frauds.

McLain, 34, was serving a 15-year sentence for interstate transport of forged or counterfeit securities. He was sentenced in September of 1973. McLain is eligible for parole at any time.

Donald Allan Walters, 31, was serving a 4-year sentence at Leavenworth for violations of Federal firearms laws. Walters was not in the computer training program at Leavenworth. He has since been transferred to the custody of a halfway house in Corpus Christi, Tex.

Emmitt Jefford, 40, was serving a 5-year sentence for car theft. On June 10, 1976, Jefford was transferred to the U.S. Penitentiary, Atlanta. Jefford, while incarcerated at Leavenworth, was not in the computer school.

Dawson's motion to have McLain, Walters, and Jefford testify was denied by Judge Earl O'Connor. It was the judge's opinion that the indictment mentioned only Frank Ready and his former wife Melinda and it was not the purpose of the trial to assess the guilt or innocence of anyone else.

NEWS MEDIA REPORTS ON READY, INDICTMENT, TRIAL

During the Ready trial, no evidence or testimony was received to indicate that the computer training program or ADP facilities at Leavenworth were used to initiate a tax scheme. However, publicity in the news media triggered by Frank Ready's indictment and trial resulted in considerable speculation outside the courtroom about the possibility that tax fraud was commonplace in the Federal prison and the possibility that the computer training project might have been a contributing factor.

For example, on August 30, 1976, Chris Drake, a reporter on the Wichita Eagle, asserted that "top level Government sources" said they were convinced that fraud was being perpetrated from the Leavenworth computer facility. Moreover, the Government sources were reported to have said the investigation of the prison had only just begun.

Drake wrote that Internal Revenue Service officials believed that prisoners at Leavenworth might have broken the IRS code on tax return auditing, enabling inmates to file false tax claims with little chance of being audited.

However, Drake reported, the U.S. Bureau of Prisons had denied that the computer in Leavenworth had been used by inmates to defraud the Government. Drake said Bureau of Prisons officials insisted that the Federal investigation into the Leavenworth situation was completed.

Drake quoted one unnamed Government official as saying, "Since the computer is only used as an educational tool, there is no way the computer could be used" by prisoners to commit crime. Charles Benson, the warden of the Leavenworth prison, was also of the opinion that his penitentiary's ADP facilities were strictly educational and had no "on-line" capability. "It would be impossible" to perpetrate a crime from the prison "because the computer is not hooked up to anything," warden Benson said, according to Chris Drake's story in the Wichita Eagle.

Drake refuted both the warden's and the unnamed official's comments by citing a Bureau of Prisons press release that indicated that the computer at Leavenworth was used by selected convicts in a rehabilitation program to process "live" data for the U.S. Department of Agriculture and other Federal agencies.

The Wichita Eagle of September 2, 1976 quoted Leavenworth Prison Warden Charles Benson as more or less retracting his earlier assertion that the penitentiary computer was not hooked up to anything. Now Benson was saying his earlier comment was based on a "misunderstanding." In addition, Bealer Gausz, the Federal Prison Industries official in charge of the computer industry at Leavenworth, was quoted in the Eagle of September 2, 1976 as saying that the prison computer was, in fact, linked directly to the Department of Agriculture's computer system.

Jim Furlong, identified by the Eagle as a spokesman for Computer Sciences Corp. of El Segundo, Calif., was reported to have said, "Leavenworth has been part of our system for at least 9 months." Computer Sciences Corp. owns Infonet. Furlong said the Infonet system spans two continents by satellite and was the main timesharing computer network used by the Internal Revenue Service, the Agriculture Department and other Federal agencies.

Thomas Dawson, Ready's defense attorney, was reported by the Eagle to have said Ready's tax returns contained mathematical formulas that appear to have been worked out by a computer.

Eagle reporter Chris Drake, in an article August 29, 1976, reported why he felt the Internal Revenue Service was particularly troubled by the Ready case and the computer training program at Leavenworth. Drake wrote that a "non-Government tax specialist familiar with the IRS system" had explained to him that IRS had set its tax return computers "with a discriminant functions program" to select tax returns that should be audited each year.

According to the unnamed tax expert, Drake reported, the IRS system enabled the computer to look at hundreds of characteristics of a tax return. Each of the characteristics is graded. For instance, Drake reported, an unusually high medical deduction might be given three points by the computer and a comparatively small deduction for a charitable contribution might be given only one point. The review of the individual return completed, the computer then tallies the points. Next, the computer submits a list of those tax returns which should be audited, Drake reported.

Drake went on to report that IRS officials feared that prisoners, by knowing just how far they could go with each deduction and still keep a low point score, could compile false tax returns with little likelihood of being audited.

On September 30, 1976, the NBC–TV Nightly News reported on Frank Ready and tax fraud in general. Ready appeared on the report as did Congressman Benjamin Rosenthal of New York. John Chancellor of NBC–TV News began the report, saying:

> We have a fascinating story this evening about taxes and tax refunds. The Internal Revenue Service each year loses hundreds of millions of dollars, maybe billions, because people don't report all they earn. But did you ever consider what might happen if someone reported that he had earned more than he really did and collected the refunds? Listen to this report by James Polk.

NBC Reporter James Polk said:

> Here in the federal prison at Leavenworth is where you might expect to find a tax-cheat, after he'd been caught, but this inmate, Frank Ready, is different. From his prison cell, the past 2 years, Ready filed eight phoney tax returns, claiming almost $80,000 in refunds. Ready collected more than $48,000 in refunds through these U.S. Treasury checks before the Government stumbled onto his scheme.
>
> Ready found a hole in the way the Internal Revenue Service checks tax returns with its computer. As a taxpayer, you file a W–2 form, showing how much was withheld from your paycheck, but the IRS fails to cross-check back against what your employers are reporting. So, on his phoney tax returns, Ready attached phoney W–2 forms listing taxes that had not been withheld from money he had not earned.

Next, Frank Ready commenting for NBC from Leavenworth, had this to say:

> The only thing they do is check the figures on the W–2 form against the figures on your return. That's as far as the check ever goes. If you're reporting income that you did not earn

> and funds that were not deducted from your money and then you turn around [and] get back the money that you have reported as being deducted. The IRS doesn't have a check and balance or a system whatsoever in order to stop that system.

Reporter Polk said:

> Ready's refund check already had been issued when he was caught by pure accident at this IRS processing center in Austin, Tex. An inspector, in a routine review of other auditors' work, found two returns with the same name and same address. Normally, the figures on your tax returns are punched through a computer, and that computer only kicks out returns for audit when tax writeoffs do not fit normal patterns. What does not go into the computer is the information companies send in on what the actual withholding was. Congress has found the IRS takes most of this company information and simply throws it away.

Now Congressman Benjamin Rosenthal of New York spoke to viewers:

> They probably lose a minimum of $½ billion to $1 billion a year, maybe more than that. The tragedy of it is that the action of these bureaucrats has been to cause a significant loss to the Federal Treasury.

Polk said, "And whatever the Federal Treasury loses, now——"

"The rest of us have to pick up the balance," Congressman Rosenthal said.

Reporter Polk concluded:

> The tax collection system in this country relies more on faith than enforcement. The case of the IRS and Frank Ready may shake that faith. James Polk, NBC News, Leavenworth, Kansas.

And John Chancellor observed:

> The IRS today said it's increased its scrutiny of individual tax returns to guard against this kind of fraud, and it said if it had enough money it would check every individual return.

CIVIL SERVICE LETTER OF SEPTEMBER 15, 1976

The committee staff's preliminary investigation of the Leavenworth computer programing industry raised questions regarding personnel practices in computer programs through the government. To obtain information on government policies and procedures in the hiring of personnel for Federal ADP programs, Senator Ribicoff wrote Robert E. Hampton, the Chairman of the Civil Service Commission, on August 27, 1976.

In his reply of September 15, 1976, Chairman Hampton said personnel security programs currently being administered in the Government were based on Executive Order 10450, as amended, originally issued in April of 1953. Hampton said Executive Order 10450 placed responsibility for designating the sensitivity of each job in a Federal agency with the head of the agency.

Hampton said that in November of 1965, the Civil Service Commission had amended Executive Order 10450 by issuing guidelines for use throughout the Government which set forth criteria to be applied in designating certain Federal jobs as "critical sensitive."

One of the guidelines issued by the Commission in 1965 said that positions identified as "critical sensitive" include jobs which involve "fiduciary, public contact or other duties demanding the highest degree of public trust." In his letter to Senator Ribicoff, Hampton went on to indicate that the committee print, "Problems Associated With Computer Technology In Federal Programs and Private Industry," issued by the Senate Government Operations Committee on June 21, 1976, had been reviewed at the Civil Service Commission.

Hampton said:

> A review of the committee print which accompanied your letter leaves little doubt that most Federal positions connected with ADP operations should be designated critical sensitive, requiring a preappointment full field investigation,

Civil Service Commission Chairman Hampton also said:

> 1. In November 1975, the Commission published guidelines for "Determining Suitability for Federal Employment." In these guidelines we purposefully avoided references to felonies and misdemeanors. Instead, we used the term "criminal conduct." Inconsistencies among the various States as to the type of criminal conduct that constitutes a felony led us to this approach.
>
> 2. The nature of the conduct is the overriding consideration in determining fitness in cases involving criminal activity, regardless of whether it is legally defined as felonious.
>
> 3. In essence, the only justification for a personnel investigation lies in its predictive value. Information gathered in such investigations should allow an evaluator to predict with reasonable accuracy whether the subject of investigation will, in all likelihood, continue an established mode of behavior. In our published guidelines considerable emphasis is placed on rehabilitation as a factor to be considered in suitability evaluations. The absence of rehabilitation—or, stated positively, the presence of recidivism—would normally result in disqualification.
>
> 4. The Commission did not formally evaluate FIPS PUB 31. We have conferred with some of our computer people who are familiar with the publication and the consensus is that it is a valuable study with sound recommendations. The Bureau of Personnel investigations has also reviewed the portions pertaining to personnel security and wholeheartedly endorses the recommendation that preemployment investigations be required on persons selected for sensitive ADP positions. The most sophisticated physical security system, without a correspondingly tight personnel security program, provides only a false sense of security. We interpret the phrase "require appropriate preemployment screening" to mean a preappointment full field (background) investigation to

establish the selectee's reputation with respect to honesty, integrity and trustworthiness.

ROBERT P. ABBOTT'S SECURITY EVALUATION

Robert P. Abbott, a computer scientist who specializes in ADP security, was retained as a consultant by the Senate Government Operations Committee to provide an analysis and evaluation of certain aspects of the Leavenworth computer operation, especially as it pertained to the Department of Agriculture.

Abbott graduated from the University of California, Berkeley, with a degree in mathematics in 1953. He is now president of EDP Audit Controls, of 7700 Edewater Drive, Oakland, Calif. EDP Audit Controls provides management and auditing services. The organization is owned by Tymshare, Inc., of Cupertino, Calif.

From November of 1971 to July of 1976, Abbott was manager of the RISOS project at the University of California's Lawrence Livermore Laboratory, Livermore. RISOS—the Research In Secured Operating Systems project—was sponsored by the Advanced Research Projects Agency of the Department of Defense at a cost of $2 million.

According to the April 1976 edition of Energy and Technology Review, published by the Lawrence Livermore Laboratory, RISOS was a special team of computer scientists assigned the task of developing methods for testing the security of data stored in computers and examining the security of selected commercial operating systems. The RISOS group, under Abbott, established major classifications of security flaws and developed both analytic tools and a methodology for evaluating the security of operating systems, Energy and Technology Review said, adding:

> RISOS was primarily concerned with the security problems of timeshared computer systems. These systems provide concurrent service to many users, generally through terminals. Under most circumstances, the results are immediately available. The central problem becomes how to keep one terminal user from illegally or accidentally obtaining data that is private to another. The computer's operating system is the vital link in this problem. . .
>
> Although the RISOS project was initiated from concerns of national security, its findings are also applicable to the issues of privacy legislation and computer-crime prevention.

Prior to his association with the RISOS project and his current position with EDP Audit Controls, Abbott served as a consultant to the Mathematical Services Corp., Oakland, from January of 1971 to November 1971; as general manager of the application division of the Berkeley, Calif., Computer Corp., April, 1970 to January, 1971; as director, Research Data Facility, Institute of Medical Sciences, Pacific Medical Center, San Francisco, May 1966 to April 1970; and as group leader, Time-Sharing Systems Group, Lawrence Radiation Laboratory, Livermore, April 1953 to May 1966.

As a consultant to the Senate, Abbott, who has retained his government top secret security clearance, was given accesss to all information and documentation obtained by the committee staff in connection with the Leavenworth situation. Then, on October 13, 1976, Abbott, accompanied by committee staff, made an inspection of the Data Systems Field Office (DSFO) in Kansas City, Mo. DSFO supports and houses the computer operations of the Agriculture Department's Agricultural Stabilization and Conservation Service (ASCS) and the Commodity Credit Corporation (CCC). The DSFO s located at 8400 Ward Parkway.

On October 14, 1976, Abbott and committee staff inspected the computer facility at the U.S. Penitentiary, Leavenworth.

Abbott's inspections of both sites were approved in Washington by appropriate officials at the Agriculture Department and the Bureau of Prisons, respectively.

On December 17, 1976, Abbott submitted a report to the Senate Government Operations Committee in which he made an evaluation of, and commented upon, security considerations he had reviewed during his October inspections.

Abbott's report is entitled, "Analysis of the Relationship Between the Programming Industry of Federal Prison Industries and the Agricultural Stabilization and Conservation Service."

In his report, Abbott said:

Findings

> F1. I am made alarmingly uncomfortable by the relationship between the Federal Prison Industries (FPI) and the Agricultural Stabilization and Conservation Service (ASCS). This feeling is due to the fact that detailed financial procedures and other fiscal operations of ASCS are revealed to a segment of our society which has demonstrated its expertise at acts of embezzelment, fraud, and other manifestations of white collar crime.
>
> F2. According to the document entitled—Longitudinal Study of the ADP Industry Participants, U.S.P. Leavenworth, 1972 to 1976:
>
> Prevention of unauthorized access thru better software and hardware improves continually. GSA recently contracted with Stanford Research Institute (SRI) to "crack" the security of the country's largest time-sharing vendor, Computer Sciences Corporation (INFONET). SRI was unable to do so.
>
> The credibility of this statement of implied security is made suspect as a result of subsequent statements by General Accounting Office (GAO). GAO indicates that the ground rules for the SRI investigation were inadequate to the task of a thorough investigation of the security features of INFONET.
>
> F3. The Department of Agriculture had completed a privacy-security review of the KCCC prior to our 1-day visit. Apparently, the basis for the Department of Agriculture review was provided by the FIPS PUB series of National Bureau of Standards and by various OMB guidelines on the implementation of the Privacy Act of 1974. A number of policies and procedures are employed by KCCC which are designed to insure the integrity of its operations.

The degree of integrity can be enhanced by the inclusion of a number of security related EDP practices which are employed by Department of Defense and by industry.

F4. The Programing Industry of FPI has established a system for teaching computer programing which minimizes the opportunity to engage in unauthorized computer related actions. Our 1-day visit did not permit a detailed investigation of the degree to which the day-to-day workings of the system conform to the statements of how the system works.

Recommendations

R1. The FPI training program, operational procedures, and unusual circumstances would be better suited to the production of computer programs involving data which is NOT related to individual privacy, data confidentiality, fiscal/financial matters, or otherwise sensitive material.

R2. It is recommended that the INFONET system be the subject of a comprehensive and in-depth EDP audit of its security features. The audit should be patterned after the procedures described in "Department of Defense Directive 5200.28M ADP Security" and the audit should include the type of procedures suggested in "Security Analysis and Enhancements of Computer Operating Systems," National Bureau of Standards, NBSIR 76-1041; April, 1976.

Whereas these two documents require full disclosure of information to the independent audit team, the process does not violate the right of Computer Sciences Corp., to protect its proprietarily developed software, procedures, etc.

R3. I would recommend that the KCCC:

(*a*) Acquaint themselves with the privacy/security concepts made available through a number of computer industry seminars;

(*b*) Institute a program of periodic inspection by an independent EDP audit group. Whether the audit is conducted by a Government group or a group from industry is incidental to the requirement of demonstrated proficiency in the EDP privacy/security audit process.

R4. The Programing Industry of the FPI would benefit greatly by:

(*a*) Beefing up their written policies and procedures;

(*b*) Implementing control procedures which not only demonstrate compliance with the policies and procedures, but which also lend themselves to the audit process.

(*c*) Institute a program of periodic inspection by an independent qualified group.

Discussion

1. My feeling of uncomfortability is based on my 5 years as originator and manager of the RISOS (Research In Secured Operating Systems) project. RISOS was instituted by the Advanced Research Projects Agency of the Department of Defense. The RISOS mission was to develop systematic methodologies for testing the security features of those DOD computers which process defense

classified information. In plain English, we were paid to be computer thieves.

A major problem in the training of staff for RISOS was to redirect their mental processes from a disposition of honesty and integrity in completing a computer programing assignment to a very negative attitude toward the computer, its operational procedures and controls. This process of thought redirection required from 3 to 6 months for even the most qualified computer professional.

The situation at Leavenworth Penitentiary is unique in that the inmates in general, and the computer industry trainees in particular, have demonstrated their prowess in counterthinking the system as demonstrated by their incarceration for embezzlement, credit card fraud, or swindles involving property or negotiable instruments. The fact that some program industry trainees are also suspected of connections with organized crime presents a picture of individuals already trained in thought processes which are contrary to those of the honest citizen.

To this situation is added an unusual opportunity to study the fiscal and financial workings of a Federal agency which regularly distributes authorizations for large dollar amounts. If we assume that the security controls within the Agriculture computer center and within the Leavenworth program are perfect, we are still left with the knowledge of a criminal mind exposed to the innermost financial workings of a key Federal agency.

There is a corresponding principle in national security matters—that of "Need to know." If you do not "need to know" certain information to perform your assigned job, then there is no reason to expose you to that certain information.

In conclusion, I should like to state clearly that my concern of discomfort is based not on computer related issues, but on the qualifications of the individuals involved.

2. The role of the Infonet system in the Programming Industry of FPI is not clear. Literature of the vendor proclaims the use of the system in the training of prison inmates. Programming Industry officials refer to the security features of the system. The same officials also indicate that inmates are not permitted to physically access the vendor supplied terminal. At issue is the efficacy of a data processing training program which forbids the type of human/computer interaction which characterizes modern day online computing.

The security features of the system are referenced both by FPI officials and by Infonet officials. The emphasis in each case is on the inability of Stanford Research Institute (SRI) to "crack" the system during an audit which was conducted at the behest of the General Services Administration. The issue here is the ability of the system to withstand unauthorized attempts to gain access to someone else's data. In view of the fact that Infonet is used by other Federal agencies, its security features are of great importance.

Further explanatory statements by Infonet officials reveal the degree of control which they exercised over what material was made available to SRI, the nature of the SRI investigation, and how much information was to be made available to the public as to the results of the audit. The entire exercise was viewed by the vendor to be at variance with the terms of the contract between the vendor and the Government.

An EDP privacy/security audit is similar to the corporate audit that any registered corporation submits to. The intent is to protect the unwary public. The Securities and Exchange Commission has made it clear that the responsibility of the CPA audit is to verify honesty in practices as well as in statements of assets. A CPA firm must examine all aspects of a corporate operation. If a corporate entity were free to specify what shall and shall not be examined, it would not meet with SEC approval.

The situation at Computer Sciences Corp. is that it exercised such control during the publicized audit. The effect is to proclaim that: "We are good because we say we are good."

Motivation for this unilateral restrictive action is a real concern to protect proprietarily developed procedures. The implication is that SRI was expected to violate client confidences by revealing closely held information. This is a position which is contrary to the fine reputation of SRI within the scientific and business communities.

Client confidence is a necessary ingredient of any professional service, whether it be law, medicine, or auditing. In fact, the intent is to expose oneself and gain the benefit of the professional expertise.

Department of Defense has been conducting EDP security reviews of sensitive computer installations for some time. Even though reports may be classified, full disclosures are made to the review team. Findings and recommendations are acted upon.

My reservations about the efficacy of the Infonet audit would be withdrawn if the audit had been conducted in an atmosphere which approximated the cooperative nature of the DOD computer security environment.

2. In visiting the Kansas City Computer Center (KCCC) of the Agricultural Stabilization and Conservation Service questions were asked according to the outline contained in appendix A of this report. The intent of the visit was to assess the security awareness, operational controls, and verification procedures of all aspects of the computer programs generated by the FPI operation.

Except for the items listed below, the policies and procedures as stated by the KCCC appear to be adequate in controlling the possibility of fraudulent irregularities in the computer operation.

(*a*) An incomplete (as compared to unsuccessful) attempt by the author of this report to gain unauthorized access to the computer room was not challenged by any employees observed to be in the immediate area. In discussions with

KCCC management, it was learned that there is no educational program to reinforce employee awareness of security related issues.

(*b*) There was no person designated to be the security officer for computer related matters. Similarly, there was no person assigned specific responsibility of implementing software security measures.

(*c*) Access control is based on validity of an account number only. Password verification is not used.

(*d*) Super Zap is a program which permits unlimited access to the most vital parts of a computer. Super Zap is used at the KCCC by the highest level programers in maintaining the computer system. Installations which are concerned about security recognize that Super Zap cannot be permitted in a situation requiring maximum protection.

(*e*) There is no procedure to debrief a terminating employee to reinforce the concepts of security as far as disclosure of information is concerned.

(*f*) Programers are required to obtain supervisor approval prior to installing a change in a programing system. There is no procedure to verify that this requirement is enforced.

(*g*) KCCC makes use of a test team concept in which the computer client and other uninvolved individuals prepare test data to be processed by the computer program. The purpose is to verify the validity of each program. This procedure applies to all the programs produced by the KCCC as well as by the FPI operation. The generation of test data, both good and bad by this process is, in the view of this auditor, incomplete. Data must be generated which tests the complete logic of the program. The generation of good and bad data is insufficient for this purpose.

3. Our visit to the FPI Programing Industry training site at Leavenworth also followed the outline as contained in appendix A. A very complete set of controls were described which are designed to control prisoner access and use of the computational resources. During our 1-day visit, it was not possible to verify compliance with the indicated procedures. More time would be required to properly assess the effectiveness of the indicated procedures and the extent to which they are rigorously followed.

DOCUMENTS

1. Memo by Phil Manuel, Dated 30 August, 1976. Subject: Background Information on Participants in the ADP Program at Leavenworth Penitentiary.
2. Study of the Chronology of the ADP Program at Leavenworth, together with documentation concerning the FPI/ADP project and its relationship to:
   (*a*) The Department of Agriculture ASCS;
   (*b*) Infonet—Computer Sciences Corp.; and
   (*c*) General Services Administration.
3. List of 157 present or former inmates at Leavenworth Penitentiary who have participated in the ADP project from June, 1972 to June, 1976.
4. Longitudinal Study of the ADP Industry Participants, U.S.P. Leavenworth, 1972 to 1976.
5. List of inmates on the Special Offenders List at Leavenworth Penitentiary as of 15 June, 1976.

6. One page document received from Warden Charles Benson on 15 June, 1976 which purports to be an accounting of all checks over $500.00 received at Leavenworth Prison.
7. Two page document received from Warden Charles Benson on 15 June, 1976 which purports to be an accounting of all Inmate Personnel Funds deposited via U.S.P. mail room.
8. FBI arrest records (rap sheets) and NCIC records on the criminal background of 45 current participants in the ADP Programming Industry at Leavenworth.
9. Reply to Senator Ribicoff, by J. Paul Bolduc, Assistant Secretary for Administration, Department of Agriculture, dated 21 September, 1976, which sets forth the terms and conditions of the interagency agreement between ASCS and FPI. This document includes the following attachments:
    - (*a*) Interagency Agreement, dated 1973.
    - (*b*) Procedures, documents and policy statements concerning relationships with ADP contractors.
    - (*c*) Description of the jobs (approximately 300) which have been sent to Federal Prison Industries for programming. Note: These descriptions include jobs which relate to general ledger, income and expense reporting, loans, etc.
    - (*d*) Computer applications for USDA-ASCS programs. Note: This listing of application systems identifies the Commodity Loans and Purchases; Loan Certification; Farm Storage and Drying Equipment Loans; Producer Payments Reporting; etc.
    - (*e*) Descriptions of the process by which various drafts are handled (e.g. Commodity Credit Corporation Control and Issuance of Sight Drafts; State and County Office Drafts; Commodity Office Drafts). This attachment also includes descriptions of various Agriculture programs (Beekeeper, Water Bank, etc.).
10. Material gathered during site visit to KCCC:
    - (*a*) DSFO Organization Chart.
    - (*b*) Concise Statement of DSFO Operations.
    - (*c*) DSFO Functional Statements.
    - (*d*) DSD Functional Statement.
    - (*e*) List of USDA Offices Located at 8930 Ward Parkway and 2400 West 75th Street.
    - (*f*) List of ADP Applications Maintained by DSFO.
    - (*g*) Employment by Occupational Skills.
    - (*h*) Newspaper Clippings Regarding Fraud With Computers.

BRIEFINGS

Five (5) briefings conducted by Fred Asselin and Phil Manuel.

SITE VISITS

Kansas City Computer Center, Agricultural Stabilization and Conservation Service; October 13, 1976.

Programming Industry, Federal Prison Industries, Leavenworth Penitentiary, Leavenworth, Kansas; October 14, 1976.

APPENDIX

AN OUTLINE FOR AUDITING COMPUTER AND DATA SECURITY

I. Policy;
II. Personnel;
III. Physical Control;
IV. Data, Programs, and Documentation;
V. Operational Controls and Policies;
VI. Back-up Computer Operations;
VII. Development of Application Programs;
VIII. Insurance of Equipment; and
IX. Security Program.

DEFINITIONS

Separation of Functions: When a process or procedure embodies more than one critical step, different individuals should have responsibility for different steps. This reduces the opportunity for collusion.

Back-up: You can be replaced: In the security context, no person should be vested with singular authority or knowledge. Similarly, planning is required for the temporary replacement of key equipment.

I. Policy

- A. Security of computer facilities
  - 1. Computer room(s);
  - 2. Remote terminals; and
  - 3. Telecommunication equipment.
- B. Protection of personal, non-public data against:
  - 1. Accidental—
    - (*a*) Modification
    - (*b*) Destruction
    - (*c*) Disclosure
  - 2. Deliberate—
    - (*a*) Modification
    - (*b*) Destruction
    - (*c*) Disclosure

II. Personnel

- A. Background verification;
- B. Penalties for falsification of application;
- C. Exit interview;
- D. Clarity of job description and assignment;
- E. Separation of functions; and
- F. Back-up.

III. Physical Control

- A. Access control;
- B. Identification of all personnel;
- C. Protection of magnetic data storage devices;
- D. Use of security guards;
- E. Reliable power systems; and
- F. Various types of protection against fire, water, and smoke.

IV. Data, Programs, and Documentation

- A. Official custodian of tapes and disks;
- B. Restrict access to storage vaults to authorized personnel only;
- C. Controls on the actions of the computer operator towards the computer operation;
- D. Quality of the documentation;
- E. Control procedures for changing critical routines;
- F. Control procedures for changes to the operating system; and
- G. Back-up for critical data, programs and documentation.

V. Operational Controls and Policies

- A. Designation of a Security Officer;
- B. The existence of audit trail information;
- C. Control of remote terminals;
- D. Proper maintenance schedule for the computer(s);
- E. Usage of passwords and other security controls;
- F. Control of the computer output; and
- G. Separation of functions.

VI. Back-up Computer Operations

- A. Availability of a back-up computer;
- B. Testing the back-up computer; and
- C. Simulation of various disaster situations.

VII. Development of Applications

- A. Generation of system specifications;
- B. Verification of system specifications;
- C. Programming standards;

D. Enforcement of programming standards;
E. Audit trail for development and evaluation; and
F. Review and evaluation.

VIII. Insurance

A. Sufficient amount to cover equipment replacement; and
B. Liability insurance.

IX. Security Program

A. Risk analysis;
B. Appropriate review of security policy;
C. Definition of privacy and security; and
D. Audit review of Compliance to policy.

INFONET DOCUMENTS

On September 14, 1976, the committee staff met in Washington with Philip A. Tenkhoff, the Computer Sciences Corporation official with responsibility for Infonet security operations. Tenkhoff was accompanied by a corporation counsel, William E. Sudow, a Washington lawyer with the law firm of Fried, Frank, Harris, Shriver and Kampelman.

The committee staff requested from Tenkhoff that Infonet provide the committee with documents indicating (1) which Federal agencies have contracts with Infonet; (2) the size, dollar volume, nature of and fees charged in connection with these Federal contracts; (3) all billings for time used and inquiries made by the Leavenworth prison computer facility; and (4) a description of physical and personnel security safeguards.

Tenkhoff and Sudow said it was Computer Sciences Corporation's intention to cooperate with the committee and that they would convey the staff's request for these specified documents to the corporation's headquarters in El Segundo, Calif.

On September 28, 1976, Sudow informed the committee staff that the requested documents would be sent to him, Sudow, within the next few days and he would transmit them to the committee. Sudow said GSA officials had been informed of the committee's staff's request and GSA had expressed no objection to turning over Infonet documents to the committee.

However, on October 18, 1976, Gail Chrzan of GSA's Office of Congressional Affairs notified the committee staff that Theodore D. Puckorius, Commissioner of GSA's Automated Data and Telecommunications Service, was of the opinion that it would not be appropriate for Computer Sciences Corporation to transmit the requested Infonet documents directly to the committee. Chrzan told the committee staff that Puckorius felt it would be desirable to have Computer Sciences Corporation first give the requested documents to GSA. Then, Chrzan said, GSA would give the Infonet records to the committee. The committee staff advised Chrzan that the Puckorius proposal, as characterized by Chrzan, was not as satisfactory as the original understanding worked out between the staff and Tenkhoff and Sudow.

Sudow then advised the committee staff that the Computer Sciences Corporation position had changed in that all requested Infonet documents would be transmitted to the committee via GSA. While voicing a protest over this procedure, the staff accepted the new arrangement and continued to express interest in having the requested Infonet documents. However, no such Infonet documents were ever given to the committee, not by Computer Sciences Corporation, not by GSA.

THE ROBINSON CASE

This staff study has already reported on the Federal Government's charge against Frank E. Ready, a convict at the U.S. Penitentiary, Leavenworth, that, while incarcerated, he defrauded the Internal Revenue Service by filing for, and receiving, an undeserved tax refund of about $20,000. It was the committee's staff's view that the Ready case, and subsequent conviction, were important because they demonstrated how tax violators could exploit the IRS computerized system of selecting returns for audit.

Two other cases will be described in this section of the staff study and the section that follows because they also demonstrate problems associated with computer technology in a large Federal program such as tax collection. Like Frank Ready, the violators in these two cases sought to exploit IRS computers.

The first of the two cases had to do with a former IRS official who perpetrated a multiple filing fraud and obtained refunds from IRS of more than $500,000. The violator's name is David G. Robinson. Thomas V. Glynn, Assistant to IRS Commissioner Donald C. Alexander, prepared a report on the Robinson case at the request of the committee staff and submitted the report to the committee.

Glynn said that on December 19, 1975, David G. Robinson of Pasadena, Calif., was arrested by agents of the Los Angeles IRS Intelligence Division on an arrest warrant issued by the U.S. Attorney in LA. Robinson was charged with having filed false claims for refunds.

Glynn said the case originated from information furnished by an IRS Intelligence Division official working out of the IRS service center in Fresno, Calif. Information developed in Fresno was that a person using the name John D. Robinson and using a newly issued social security number had filed four separate income tax returns claiming refunds totalling $653,279. Glynn said records from the Fresno IRS center indicated that three of the claimed refunds totalling $565,340.31 had been mailed to John D. Robinson.

Each of the returns filed by Robinson included W-2 forms marked "Duplicate." Glynn said the W-2 forms showed John D. Robinson to be an employee of Lomas and Nettleton, Post Office Box 1328, Houston, Texas. Glynn said investigation revealed that John D. Robinson was not an employee of this firm and that the firm's W-2 forms were different than those supplied by Robinson.

The mailing address given by Robinson was the business address of a telephone answering service. The answering service also allowed clients to use its address as a mail drop if they wished. Intelligence agents were able to identify David G. Robinson as using this address as a mail drop. Postal authorities helped IRS agents find Robinson's residence, Glynn said.

IRS agents learned that David G. Robinson used the name John D. Robinson as an alias. They also learned that David G. Robinson had once been a revenue officer for IRS in Los Angeles. A criminal record was also uncovered, Glynn said, as Robinson was found to have been arrested in 1973 in Australia by IRS agents. Robinson had fled to Australia to escape being charged with embezzlement. The charge was related to his employment as a revenue officer. Glynn said Robinson was extradicated from Australia, tried, convicted and sentenced to 1 year and 1 day in prison. Robinson served a 30-day sentence for a Federal firearm conviction in May of 1975, Glynn said. He was also found to have filed false information with the Treasury Department's Bureau of Alcohol, Tobacco, and Firearms.

IRS agents determined that Robinson's 1975 residence—his home at the time of his tax fraud arrest—cost the former revenue officer $84,500, a sum Robinson paid in cash. Glynn said that among Robinson's possessions at the time of his arrest were four Jaguar automobiles, a Ferrari, a Lamborghini, a Mercedes Benz and a Beechcraft aircraft.

Exemplars of Robinson's handwriting were used to identify his signatures on the four false tax returns and the three refund checks he received and cashed. Robinson plea bargained and, on January 27, 1976, he was given a 5-year prison term. Glynn said that Robinson agreed to help the Government recover the $565,000 in refunds. Robinson is currently incarcerated at the U.S. Penitentiary, Terminal Island, Calif.

Glynn said that it was "obvious" to IRS that Robinson, as a former employee, had "some knowledge of the inner workings" of IRS and this was to his advantage in trying to carry out his frauds. But, Glynn said, IRS employees do not usually have complete knowledge of how the Service functions. He noted, for example, that the internal controls that triggered the identification of the questionable John D. Robinson tax returns were not known to David G. Robinson.

Glynn did say, however, that IRS personnel had studied the scheme used by David G. Robinson and "we are taking steps to improve refund processing controls in an effort to detect this type of case prior to issuing refunds." It should be noted that in both the *Ready* and *Robinson* cases—and in the case that will be described in the next section of this staff study—the violators were caught but only after they had received and cashed their refund checks.

Glynn said:

> In summary, the returns filed by Robinson passed through normal processing procedures, and refunds for the years 1972 through 1974 were issued. Post processing refund controls identified the returns as being potentially fraudulent and the matter was referred to the Intelligence Division for investigation. The investigation proved the returns to be false and the suspect was identified and arrested by the Intelligence Division.
>
> An analysis of 24 false claim cases that occurred between 1973 and 1975 indicates that our internal controls are effective in detecting false refund claims. These 24 cases involved 923 returns with false claims totalling $2,364,758. Three of the cases involved employees, one involved the former employee in question [David G. Robinson] and 21 involved the general public. In these cases we prevented $1,317,504 from being refunded because early processing tests or controls identified the returns as being fraudulent. The others

> were detected by post processing controls, as in the Robinson case.
>
> In processing refund claims, we are concerned with making timely refunds. Therefore, the processing controls are designed to detect refunds with obvious questions that can be resolved without undue delay. Post refund controls require additional inquiry and analysis, some of which can only be made after processing is completed. False claims represent a minute portion of refund claims and delays of refunds in general would unnecessarily inconvenience the general public.

In his report to the Senate Government Operations Committee on the David G. Robinson tax fraud case, Thomas V. Glynn, assistant to IRS Commissioner Donald C. Alexander, did not use the word "computer" once. But it was the IRS computerized system for evaluating tax returns that Robinson sought to exploit, enabling him to carry out his tax refunds scheme. Moreover, according to a May 18, 1976, article in the National Enquirer purporting to be an interview of David G. Robinson, the former IRS revenue officer is quite candid about how he tried to compromise the IRS computers.

Robinson is reported by the National Enquirer to have said from his cell in the Federal prison at Terminal Island:

> I cheated Uncle Sam's tax computers out of more than half a million dollars in hard cash—and I could do it again any time I want.
>
> It was easy. I knew exactly how the IRS computers work. I found major loopholes in the system that could have landed me massive sums of money . . . had it not been for the most unexpected piece of bad luck.
>
> For this little caper, I created a completely mythical character. I named him John D. Robinson. I gave him an authentic address. I got him a social security number. I got him business connections.
>
> Over a 6-month period starting in early 1975, I sent in tax forms for Robinson for the previous 3 years, with phoney W-2 statements. The IRS computers got to know Robinson . . . he became a person in the computer's memory.
>
> Then I decided it was high time good old John D. Robinson should start getting some hefty tax breaks. And this is where things get tricky, because when you fill out tax forms for the purpose of fraud, they have to be exactly perfect. But they went through the computer like a dream.
>
> Over a 2-month period, the computer sent Robinson three great big fat checks—for $180,000, $186,000 and $196,000. All I had to do was take them to the bank and pay them into the account I'd opened for J.D. Robinson, then draw out the cash.
>
> I opened my own air charter business, bought an $84,500 home, a private airplane and seven cars—three Jaguars, a Ferrari, two Lamborghinis and a Mercedes.
>
> We entertained lavishly. We often drank 250-year-old bottles of Remy Martin brandy, costing $550 each.

> We were living the good life and it didn't look as though anything could end it. I was busy making plans for further IRS ripoffs.
>
> The whole thing came crashing down last December 19 [1975]. The agents came to pick me up at my office in Irvine, Calif.
>
> My wife was with me and we dodged out the back door, leaping into our Mercedes sports car with the agents in hot pursuit. We made it to the local airport and took off in my private plane. We flew to Orange County airport where we had another car parked, then drove to my home—where the agents caught up with us. The game was up.

The same National Enquirer article also quoted an assistant U.S. attorney, A. Howard Matz, as saying, "Don't think anybody else can do this because the entire IRS has already implemented measures to prevent this type of refund fraud from occurring again."

The article identified Assistant U.S. Attorney Matz as being with the Fraud and Special Prosecutions Division of the U.S. Attorney's Office, Los Angeles. Matz, the article said, "coordinated the intensive investigation conducted by the IRS" into the David G. Robinson tax fraud.

THE GHOLSTON CASE

Betty Marie Gholston, 41, and her daughter, Venita Huffman, 23, both of the Detroit area, pleaded guilty to charges of fraudulent negotiation of tax refund checks in arraignment proceedings in U.S. district court in Detroit on December 6, 1976.

On December 10, 1976, the U.S. attorney in Detroit, Philip Van Dam, announced that the guilty pleas by Gholston and Huffman were the result of an investigation in which Federal agents had broken up a tax fraud conspiracy in the Detroit area that had already defrauded the U.S. Government of at least $250,000.

Again, it was an IRS computer which had been outsmarted by violators. Ironically, even though the ring, reportedly led by Betty Gholston, had been broken up, Federal authorities believed more IRS refunds for Mrs. Gholston and her accomplices would continue to be mailed. "Betty kept very careful records of returns she sent in," U.S. Attorney Van Dam said. "We know there are more checks in the works. IRS tells us there's nothing they can do about it."

Detroit Free Press reporter Helen Fogel, summing up the Government's dilemma, wrote of the Gholston case December 10, "Meanwhile, the IRS computer still is spitting out refunds."

Betty Gholston a receptionist and part-time tax preparer, was reported by the Free Press to have led the gang of tax violators who had participated in the filing of hundreds of fake IRS returns that resulted in refund checks being sent to Gholston and her accomplices. The tax returns had fictitious names but real social security numbers and legitimate employer identification numbers.

According to the Free Press' Fogel, information developed by the U.S. Secret Service led law enforcement agents to uncover the Gholston scheme.

The staff of the Senate Government Operations Committee asked U.S. Attorney Philip Van Dam to give the committee a statement on the Gholston fraud.

In his statement sent to the committee on December 20, 1976, U.S. Attorney Van Dam said:

> The investigation presently being conducted in the eastern district of Michigan by the U.S. Secret Service, the Internal Revenue Service, and the U.S. Attorney's Office reveals that beginning in 1972 and continuing to the present time, a large-scale fraud has been perpetrated against the U.S. Department of the Treasury. As this investigation is still in progress, only a fraction of the evidence has been compiled; therefore, the estimates contained herein are inconclusive.
>
> In 1972, Betty Gholston undertook a scheme to defraud the Federal Government through the submission of false income tax returns. Mrs. Gholston recruited friends and acquaintances to assist her in this scheme. With her experience in tax preparation, Mrs. Gholston had the basic expertise needed to prepare income tax returns.
>
> The scheme is really very simple. Mrs. Gholston would make application to the Social Security Administration using a false name and birth date. Pursuant to the application, a social security number would be issued and the social security card would be mailed to the address of Mrs. Gholston.
>
> Next, Mrs. Gholston would obtain blank W-2 forms from an office of the Internal Revenue Service. Using the false name, the social security number provided by the Government and a genuine employer identification code, Mrs. Gholston would fill in the information on the W-2 form. She would also supply the income tax information and the withholding information on the W-2 form. Finally, Mrs. Gholston would fill out a 1040A and in each such form provide a claimed refund of anywhere from $300 to $500 and would mail the completed forms to the Internal Revenue Service.
>
> Upon receipt, Internal Revenue Service would process the refund claim and issue a check to the address noted on the 1040A form. (The addresses supplied by Betty Gholston were either her own address or those of relatives or friends.) When the refund check was received, it would be cashed by an accomplice of Mrs. Gholston, or Mrs. Gholston herself. The checks were deposited into bank accounts set up in the name of nonexistent corporations or businesses. Moneys deposited in these accounts would later be withdrawn by Mrs. Gholston or one of her associates.
>
> To date, the investigation has revealed that approximately 300 social security numbers were obtained and used in the preparation of fraudulent income tax returns. Also, approximately 30 addresses were used on the 1040A's and the refund checks would be mailed to those addresses.
>
> It is estimated that the scheme resulted in the issuance by the Internal Revenue Service of approximately 500 refund checks in the amounts of between $300 and $500 per check.

In addition to the scheme set forth above, investigation by the Internal Revenue Service developed a similar situation taking place on the East Side of Detroit. This scheme involved the submission of claims for refunds to the Internal Revenue Service using names and social security numbers of welfare recipients. The refund checks would be mailed to various addresses on the East Side of Detroit and then turned over to the subjects in the investigation. Fifty-eight submissions were made to IRS for refunds of approximately $2,400 per submission. Before the scheme was uncovered, 14 checks totaling $36,000 were mailed to the addresses used on the 1040A's and the checks were cashed by the subjects.

All of the 58 submissions were determined to be fraudulent.

It is apparent that safeguards are needed within the processing of the refund claims with the Internal Revenue Service in order to prevent future frauds against the Government, for instance: (1) Before a refund is made to any individual using a certain social security number, a check should be made to insure that taxes were paid by an individual using the social security number and that the withholding was at least as much as the claimed refund; (2) No refunds should be made for taxable years prior to the date of the issuance of the social security number; (3) Periodic checks should be made when it is determined that more than one refund check is being mailed to a specified address in any one taxable year; (4) All late filings or any refunds should be closely scrutinized; (5) Any questionable refunds should be immediately turned over to the local office of IRS for investigation.

It is inconceivable that schemes such as those developed in the eastern district of Michigan would be allowed to continue. The simplicity of the schemes underline the possibility that similar frauds are being perpetrated in other districts throughout the Nation.

THE SECOND CIVIL SERVICE COMMISSION LETTER

Robert E. Hampton, Chairman of the Civil Service Commission, said in a September 15, 1976 letter to Senator Ribicoff that Commission officials had reviewed the Senate Government Operations Committee Print of June 21, 1976, "Problems Associated With Computer Technology In Federal Programs and Private Industry," and now felt that Government employees working in sensitive computer programs should be subjected to a background check before being cleared for the job.

On December 27, 1976, Hampton sent a second letter in which he summarized the Commission's views on personnel security in Federal ADP programs. Chairman Hampton also expressed the opinion that background checks should be required only for those personnel who would be working in the national security field, in projects having to do with personal privacy and certain aspects of the economy, and in programs that resulted in the distribution of taxpayer's money.

Hampton wrote:

> Concerning my letter to you of September 15, I would like to clarify my reference to the need for critical sensitive designations for positions connected with ADP operations. It would be unrealistic and unnecessary, I believe, to attempt to apply such a designation to casual or routine roles in computer based operations. Rather, the positions that should call for careful consideration of the application of critical sensitive standards should be those involving access to national security information, those offering the opportunity to divert highly private or economically valuable data, and those concerned with the distribution of funds.

Hampton then went on to summarize the three principal Civil Service Commission findings on personnel security in Federal programs. Hampton said the Commission's findings, in summary, are:

> Positions in Federal computer programs are not generally designated as critical sensitive per se.
>
> Contractors may by contract terms and conditions be required to provide for proper security in the operation of ADP systems. These procedures could include personnel standards and must include such standards when the Privacy Act applies.
>
> There are no mandatory Federal security standards for computer positions except for those requiring access to classified information. However, the Brooks Act, Public Law 89–306, would seem to authorize the development of such standards.

Hampton also noted:

> The personnel security/suitability standards for Federal employees are contained in part in [Executive Order] 10450 and the standard for granting access to classified information is contained in Executive Order 11652. Under Executive Order 10450 the head of each executive agency designates the sensitivity of positions in that agency. Some agencies such as the Energy Research and Development Administration have been specifically given security by legislation over non-Federal or contractor positions. Also, the Department of Defense administers a huge industrial security program under Executive order authority. Finally, the Privacy Act . . . mandates that for systems of records subject to the Act that agencies establish rules of conduct for persons involved with the operation of these systems, that they instruct these people on the rules and requirements for security, and that they establish appropriate administrative, technical, and physical safeguards for security and confidentiality. This would apply to contractor personnel of the agency. Furthermore, procurement law would permit the inclusion in contracts of clauses designed to insure the appropriateness of contractor personnel and the adequacy of security provisions. The Commission, in its personnel security appraisal program, advises agencies concerning position sensitivity classification.

The Commission has no authority with respect to non-Federal positions.

In researching some of the matters raised in your letter we contacted several agencies which have major computer facilities. We find that these agencies have not designated computer related positions as critical sensitive for the most part; this means that a preappointment full field investigation is not a requisite for employment. The notable exception is DOD where multiple entry computers containing national security information necessitates critical sensitive classification for users.

V. INDIVIDUAL AGENCIES COMMENT ON COMPUTER PROBLEMS

The staff of the Senate Government Operations Committee sought to obtain information on computer security practices and problems in several executive branch agencies, including the Central Intelligence Agency, the Department of Defense, the Department of Justice, the Federal Bureau of Investigation, and the Department of Health, Education, and Welfare.

THE CENTRAL INTELLIGENCE AGENCY

The committee requested assistance from the Central Intelligence Agency. It was the staff's view that information from the CIA regarding computer security would be helpful in learning how an agency with very high security standards dealt with the problems of securing its own computer systems against compromise and other forms of unauthorized access. Meetings were held attended by CIA personnel and committee investigators in which agency spokesmen cooperated with the request, expressed by Senator Ribicoff in his May 21 letter to CIA Director George C. Bush, to have the agency comment upon the three reports issued in the spring of 1976 by the General Accounting Office on problems associated with computer security in Federal programs.

During the meetings with CIA personnel and in letters written by Senator Ribicoff to CIA Director George Bush, it was asserted that the preliminary staff inquiry was focusing, in part, on what Government standards should be regarding the hiring of personnel in Government computer programs and the personnel employed in computer programs conducted by commercial firms under contract to the executive branch.

Independent inquiry by the committee staff had indicated, the CIA was advised, that the CIA was one of the few agencies in the Federal Government, if not the only agency, which required personnel to be cleared at the top secret level to have access to computer systems as well as all other systems and facilities. It was the staff's information that this requirement, coupled with the need to know limitation, was designed to provide maximum security against compromise.

In writing, the committee staff advised the CIA that the CIA "mission is unique within the Government. That being said, though, does it seem practicable to you that a similar system of clearance and need-to-know limitations could be imposed in other agencies in connection with computer applications only? In other words, are security precautions applicable throughout the CIA capable of being applied in computer security operations in other Federal operations? In turn, is the concept realistic enough to be pursued any further? Or is it your judgment that, owing to differing objectives, procedures, and overall work style, there would be little to be gained by an effort to have other agencies emulate yours in the computer field?"

Next, the committee staff raised the issue of security indoctrination. The staff asked if the CIA could explain the general procedures the agency followed when introducing personnel to security considerations concerning computers. In addition, the staff noted, the CIA's practice of making security indoctrination a continuous process may be one that other agencies may wish to give consideration to in the computer field.

The Senate Government Operations Committee staff requested information from the CIA on its practice of instructing personnel on computer security safeguards on a continuous basis. In addition, the staff learned, CIA placed its entire computer program under continuous scrutiny by a group of computer security officers. The CIA was asked if such a system, in altered form, could be applied in other agencies. The question was asked, Does an agency have to assume certain of the CIA's high-intensity security characteristics in order to provide adequate security safeguards? Or is it possible to deploy several CIA procedures—the computer security officers mission, for example—on a selective basis?

The committee staff pointed out that from its own preliminary evaluation of the CIA's approach to security it was determined by the staff that the CIA operates in general on the assumption that not only is there potential for compromise in any ADP system; it is also likely that an attempt will be made to effect that compromise. The committee staff asked for the comments of CIA officials as to the desirability of seeking to instill that manner of thinking into agencies outside the national defense and intelligence communities. The staff was particularly interested in knowing if more strict security standards could be used in those agencies which, while not having a national security mission, do have responsibilities that rely on computer systems which process financial transactions leading to disbursements of large amounts of public funds.

The committee staff called to the attention of the CIA a Senate executive hearing before the Senate Foreign Relations Committee. The hearing, held January 14, 1949, was made public in July of 1976. The testimony the staff cited was given by the late Dean Acheson. The document referred to is entitled "Executive Sessions of the Foreign Relations Committee (Historical Series)," volume II, 81st Congress, first and second sessions, 1949–50.

Testifying in connection with his association with Alger Hiss, Mr. Acheson discussed overall security problems within the executive branch. On pages 10 and 11 of the hearing volume, Mr. Acheson made comments which, the staff felt, had relevance to this committee's preliminary inquiry into computer security.

Mr. Acheson testified:

> During the war, documents of the greatest security, which were prepared in the War Department and were sent over to the War Production Board, we now discover in the captured files of the German Secret Service. How they got

> there—every single effort of the FBI and everything else has been put on this, and no results have come up.
>
> Security is an extremely difficult thing. My own suspicion of it is that people who are really conducting spy work for foreign governments do not fool with exposed people like high officers of the Government. I think what they do is to work through much more minor characters—stenographers, or janitors, or char women, or somebody who can get hold of something of that sort. I don't say they never approach high officers of the Government, because they apparently have, as you have seen in these records, but I imagine that their real paydirt comes at a lower level.
>
> But, as I say, the efforts have not been very rewarding in finding out how this thing happens. Security measures are being taken. This has been a problem which we have had for a very long time and it is a very worrisome problem.

In connection with Mr. Acheson's testimony, the CIA was asked to provide some commentary on the late Secretary of State's assertion that it is often lower level personnel who are frequently the targets of security penetration efforts. The CIA was asked if its own officials concurred in Mr. Acheson's views and then was asked to offer its own ideas on how other executive branch agencies, as well as private industry, might seek to control this problem as described by Mr. Acheson. The staff went on to say that its own independent inquiry had indicated that the CIA was acutely aware of the computer security problem associated with lower level personnel.

Similarly, the General Accounting Office, in its April 27, 1976, report to the Congress, "Computer-Related Crimes in Federal Programs," had made the point that most of the cases of computer compromise GAO had examined did not involve sophisticated attempts to use ADP technology for fraudulent purposes; rather, GAO said, attempts at compromise were often uncomplicated acts not requiring a high degree of knowledge about computer technology. Donn B. Parker, of the Stanford Research Institute, in his report on computer system compromise in private industry, also noted that frequently the criminal violators did not hold very senior positions within the firms they stole from.

On November 10, 1976, George Bush, the Director of the Central Intelligence Agency, wrote to Senator Ribicoff to respond to points raised during this preliminary inquiry into problems associated with computer technology in Federal programs and private industry.

Director Bush told Senator Ribicoff that he shared the Senator's concerns in the area of computer security, computer fraud, and automated decisionmaking computer applications. Bush said that from his own Agency's point of view the compromise of a computerized information system can have dire consequences. He added, however, that:

> Fortunately, the fundamental security awareness of the Agency since its inception to protect its operations and its firmly established security concepts and programs, formed a solid basis upon which the agency's security of its computer operations has been built.

As did other Government officials who assisted the committee in this inquiry, CIA Director Bush stressed the importance of personnel security—that is, of recognizing that no system, no matter how physically secure, can be truly secure unless the personnel who work with it can be trusted. Accordingly, Bush explained, a basic underlying concern at the CIA is the trustworthiness and integrity of personnel who have access to classified computer systems and to the information contained in them. "No measure of technical and physical security will assure protection if the personnel involved are not of proven reliability," Director Bush said. He said this principle would apply to all persons having access to computers regardless of their level of responsibility.

Bush said CIA officials involved in security matters were in agreement with the late Dean Acheson's 1949 testimony before the Senate as it related to low-level personnel being frequent targets for security penetration.

Bush said the belief that, "Foreign governments concentrate more on compromising low-level personnel rather than high level officials" found support in the espionage cases of Sergeants Jack Dunlap and Robert Johnson. Dunlap was a U.S. Army sergeant assigned to the National Security Agency from 1958 until 1963 when his espionage activities were uncovered. He committed suicide prior to the completion of the investigation. While at the National Security Agency, he served as a chauffeur and as a messenger. Johnson was a staff sergeant (E–6) in the U.S. Air Force assigned to the Armed Forces courier service. He had been recruited by the Soviets in the early 1950's and was assigned to Orly, France, as of 1964 when his espionage activities were uncovered. He confessed to espionage in 1965 and was subsequently tried and convicted. Bush said his Agency's own experiences in security affairs confirmed, "the maxim that all levels of positions must be included in any effective security program." Moreover, Bush said, even when such human reliability is established, access to information must be controlled "on the basis of strict need-to-know to limit any resultant damage should someone having access later prove to be untrustworthy."

The Senate Government Operations Committee staff had hoped that Bush would make recommendations, or suggestions, as to how, from his Agency's own experience, other Federal departments could strengthen their own computer security safeguards. As the staff had said several times to CIA personnel in the course of the preliminary inquiry, it seemed to be a worthwhile goal of trying to apply certain ADP security techniques which had evolved at CIA to other Federal programs where the issue may not be national security but at stake were considerations of nearly equal consequence, such as individual privacy data and computer systems which process financial transactions leading to disbursements of large amounts of public funds.

In response to the staff's request, Director Bush made clear that he did not consider it desirable for other agencies to look at the CIA for leadership in the computer security field. "Our comments are general since, as you undoubtedly understand and appreciate, the Agency cannot for obvious reasons discuss in detail the security methods used to safeguard computer operations," Bush said, adding, agencies, since the degree of protection afforded must be determined by the degree of sensitivity of the information to be protected. Each department and agency responsible for the protection of its information must make its own judgment in this regard."

Bush's response lent credibility to the staff's preliminary finding that in projects relating to national security the executive branch will not hesitate to take appropriate steps adjudged to be called for in securing an information system and thereby achieving successful completion of a mission. Conversely, however, in the computer field, civilian offices of the executive branch tend not to spend the resources needed to achieve reasonably secure information systems. It is true that national security considerations are vital to the survival of this Nation and all information systems relating to the Nation's survival must have a high priority regarding security. It was the staff's view, though, that along with national security considerations, other Federal projects—projects concerned, for example, with the health, education, and welfare of the American people, projects relating to Federal taxation and farming policies—which rely to a considerable extent on computer technology should also have the benefit of sound security procedures. Some of these sound security procedures could be in place in the CIA, for example, and it was the committee staff's view that certain techniques evolved by that Agency might be, under certain circumstances, applicable to nonnational security Federal programs. However, CIA Director Bush seemed not to share this view, noting that his own Agency's security procedures should not be used as a model for other Federal programs.

In specific terms about CIA security procedures, Bush said the authority for his Agency's computer security program is based on the general authority for the security of the CIA as set forth in statute and Executive orders. The National Security Act of 1947 (50 U.S.C. 403) section 102(d)(3) placed the responsibility upon the Director of Central Intelligence for the protection of intelligence sources and methods, Bush said.

This responsibility, Bush said, is also expressed in section 6 of the CIA Act of 1949 (50 U.S.C. 403g). He said the CIA's program was also governed by the Privacy Act of 1974 which provided "strict guidelines for the proper protection of the storage of personal information" and of Executive Order 11652. This Executive order, named "Classification and Declassification of National Security Information and Material," established policy for the protection of classified information, Bush said. Bush said another Executive order, No. 11905, "United States Foreign Intelligence Activities," section 4(a)(8), established the responsibility of the Director of Central Intelligence to provide policy and guidance to the intelligence community agencies for the protection of intelligence sources and methods.

Bush said the CIA's computer security program was formalized in 1967 "as a unique security discipline" with the appointment of a Special Assistant for Automatic Data Processing within the Office of the Director of Security. Bush said additional staffing was provided as the CIA's computer operations advanced and grew. At the present time, Bush said, the information systems security group of the Office of Security develops and promulgates computer security policy, assists in implementation of this policy and, through a continuing review of computer operations, acts as an enforcement body.

Bush said the information systems security group is staffed by both professional security officers and professional data processing personnel. Bush said a professional security officer is also assigned to the Office of Data Processing. "This personnel mix provides for the best interchange and understanding of the complex computer security problems and solutions," Bush said. "In addition, this staffing for computer security allows responsiveness to the diversity of computer operations and security requirements." It should be noted that CIA's mixing of security personnel with ADP experts, as described by Bush, is along the lines of a major recommendation by the General Accounting Office that strongly urged all Federal agencies with ADP systems to use computer personnel with security personnel in arriving at a computer security policy. In its report of May 10, 1976, "Managers Need To Provide Better Protection for Federal Automatic Data Processing Facilities," GAO said:

> Management officials [should] be appointed at Federal installations having data processing systems and that they are assigned responsibility for ADP physical security and risk management. Such officials should be aware of the impact of ADP operations on the organization mission or goals and the importance of data and records to U.S. citizens and the Federal Government. Also, the official should be knowledgeable in data processing and security matters.

CIA Director Bush said his Agency's security program is a combination of the "traditional security concepts of personnel security, physical and technical security, and procedural security, with computer hardware, software, and data security." These concepts and their implementation result in a selection of personnel with high integrity combined with procedures establishing legitimate and authorized access and use of the computer and its resources, Bush said.

Protection of information is a primary goal of CIA security, Bush said, noting that computer security is one aspect of the CIA's overall security environment. Bush said, "The computer, as a processor or handler of information, must therefore be protected at the same level as the information it is processing." Bush went on to say that high security standards are required because of the storage and availability of large quantities of information within a computer system and the relative ease with which this information can be retrieved and manipulated without appropriate controls.

Bush said:

> The unique mission and environment of the CIA have required the establishment of high security standards for all its activities to protect against hostile penetration or destruction.

Bush then described specific security safeguards at the CIA which have direct relevance to the computer security program. He discussed personnel security first, saying:

> Historically, the agency has always placed a great deal of emphasis on personnel security—all applicants are subject to a background investigation and polygraph examination to establish that they meet Agency security criteria. These criteria require that all employees be of excellent character, and of unquestioned loyalty, integrity, discretion, and trustworthiness.

Bush said that all CIA personnel must meet the requirements for a top secret clearance. Bush said because all CIA employees are cleared top secret the agency thereby strives to guarantee a high standard of personnel security for all employees used in computer operations. In addition, he said, the CIA has a program under which employees are periodically reinvestigated to confirm that they continue to meet the same high standards as when they joined the Agency. Bush said that the CIA's personnel security program applied to all employees, no matter what their grade or position. "This insures," he said, "that there is no one group of employees which is any more vulnerable to security compromise than any other group."

Bush said the CIA maintains a high degree of physical security for all its installations. He said that physical security can be viewed as "protective rings or barriers surrounding an asset." He said that as the value of the asset or, conversely, the assessment of a perceived threat varies, so will the strength of the physical security of the asset. Bush said the nature of a computer facility in both value of equipment and data, establishes a high degree of physical security protecting these areas, according to the CIA approach to security. Bush said examples of physical security features the CIA uses are physical locations, vaulted areas, controlled access, alarms and established security procedures.

Bush said that the computer hardware and the software utilized to operate them at the CIA had been designed to provide certain forms of self-protection for the computer systems and the data stored and processed by them. Bush said the CIA employed these protective features, where applicable, as an important and valuable security tool. Bush said that when evidences of computer vulnerability were detected, there was a "commensurate demand for security, and the computer hardware and software security features are appropriately emphasized."

Bush said that security indoctrination and education of all employees was a continuing process. Bush said computer users were additionally provided security indoctrination through briefings, documentation, and notices concerning various computer security problems and features.

Bush said that in addition to the computer security program at the CIA, a special computer audit group within the ADP audit staff was established in 1969. The ADP audit staff reports to the CIA Inspector General, Bush said. Initially, he said, the special group within the ADP audit staff focused its attention on automated computer systems in CIA's administrative areas. Examples of concern to this group were ADP systems relating to payroll, general accounting, inventory control, and personnel, Bush said. Now, however, Bush said, the CIA had decided to extend this group's audits to other major computer systems in the agency. The expansion of this special audit group will be implemented "as personnel become available," Bush said. He said that in addition to periodic review of individual systems, the special ADP audit group would conduct audits of individual computer installations in the CIA "to insure proper management controls over computer technology."

Bush said that discussions with ADP auditors and managers in private industry and other Federal agencies, including GAO, had convinced CIA officials that their approach to ADP auditing is adequate. Bush said ADP auditors at CIA monitor computer systems during design and development as part of a team. This team, Bush said, included representatives of the end user, the ADP professionals, and an ADP auditor. Bush said CIA auditors and ADP professionals agree that it is more difficult and costly to correct built-in weaknesses after a system is operational than to eliminate the weaknesses in the progressive stages of development and testing.

Bush said:

> CIA's program, then, is based on a close working relationship among a group of trained and responsible ADP professionals, an independent group of computer security professionals, and an independent group of ADP auditors. This ongoing program is continually monitored and improved to insure that it remains effective. CIA is confident that this program provides reasonable safeguards against the computer abuses covered in the recent GAO reports.
>
> Due to its unique mission and environment, the costs of the Agency's security program are accepted as necessary. The computer security program is an integral part of the Agency's overall security program, and it is extremely difficult to cost out this as a separate program other than on a personnel basis. Overall cost factors would, however, at a minimum include personnel clearance, physical security, computer hardware and software, safety and contingency plans, and personnel costs. These specific costs are dependent on the requirements for protection of an asset and its worth.
>
> The Agency's computer security program is based on the value of assets, estimation of the threat to these assets, and a management commitment to protect these assets against threats. The program is not a static one but rather could be described as dynamic, attempting to advance and improve as the computers with which it is involved advance and improve.

Demonstrative of the CIA's concern over matters relating to computer security were preliminary steps taken by the agency prior to having any discussions at all with committee staff investigators. Even though it was strongly asserted by the staff that the inquiry as directed by Senator Ribicoff was not to pursue matters that would in any way impact upon national security considerations, CIA spokesmen said they would conduct preliminary discussions with the committee staff when it was demonstrated that the staff investigators with whom they were to meet had Department of Defense top security clearance. Once it was established that the committee investigators did have such clearances the discussions were held.

DEPARTMENT OF DEFENSE

Senator Ribicoff asked Secretary of Defense Donald H. Rumsfeld to give the Senate Government Operations Committee a statement spelling out the Department's views and responses to the issues of computer security and computer crime. Joseph P. Welsch, Deputy Assistant Secretary of Defense for Management Systems, was designated to prepare the Department's statement. The statement was submitted to the committee on December 3, 1976.

Addressing his comments to Senator Ribicoff and other members of the committee, Deputy Assistant Secretary Welsch had this to say:

> There has been a great deal of attention and concern directed towards computer abuses, reliance on computer systems for decision making and the vulnerability of today's computer technology to unauthorized penetration. I believe that this concern is valid and I share it. The GAO reports have helped us identify and focus on these problem areas. I am confident that your interest will provide another opportunity to explore these problems and help in developing suggested actions for their resolution.
>
> I would like to confirm our awareness of many of these problems, the policy and management actions that exist or are being put into motion to counteract them and our planned efforts to develop the necessary procedures and technology to more adequately address them. I have no doubt that solutions are forthcoming. The immediate challenge is to protect national security information, prevent computer abuses and insure that individual privacy is maintained while improved procedures are being developed.
>
> The automatic data processing (ADP) program within the Department of Defense (DOD) has been a formally identified program for many years and was revised to incorporate the provisions set forth in Public Law 89-306 "The Brooks bill". The DOD ADP program reflects the policy guidance provided by the Office of Management and Budget (OMB) and the General Services Administration (GSA), as well as the technical guidance provided by the National Bureau of Standards (NBS). The senior Defense Official responsible for the ADP program is the Assistant Secretary of Defense (Comptroller) who establishes DOD ADP Policy guidance (Figure 1).[1] My primary discussion will serve the Comptroller's responsibilities for general purpose ADP systems which are the subject of your letter of June 29, 1976.
>
> To advise the ASD(C) on ADP management issues, an ADP Policy Committee chaired by the Deputy Assistant Secretary of Defense for Management Systems has been established. This committee, which is composed of senior officials from the various OSD staff offices, the military

---

[1] Figures 1 through 10 are printed here beginning on p. 164.

departments, and the Defense agencies, meets quarterly to address issues of concern to management.

Each of the military departments and Defense agencies has a senior ADP policy official who oversees the execution of Defense ADP policies in his respective organization. Within the military departments, the Assistant Secretaries for Financial Management perform this function. This is illustrated in figures 2, 3, 3A and 4. The senior ADP policy official in the Defense Agencies is typically an Assistant Director. For example, in the Defense Supply Agency, the Assistant Director for Plans, Programs and Systems (figure 5) performs the ADP policy function.

The military departments and the Defense Supply Agency have established central systems design and development activities and central ADPE selection activities. The major design and development activities are listed in figure 6 and the ADPE selection activities in figure 7.

The ASD(C) and the senior ADP policy officials of the military departments and Defense agencies receive assistance from the various functional areas on policies and practices that affect the ADP area. For example, policies addressing the protection of classified and personal information; contingency planning; telecommunications; research and development; and the like are provided by the respective functional organizations. Where there is an impact upon ADP, the policies are coordinated with the ASD(C).

DOD ADP policy covers a broad spectrum of management concerns. The Defense ADP program is based on three policy directives. The first is DOD Directive 5100.40, "Responsibility for the administration of the DOD automatic data processing program," August 19, 1975, which designates the Assistant Secretary of Defense (Comptroller) as the senior DOD ADP policy official and outlines the responsibilities for administering the DOD ADP program. The second is DOD directive 4105.55, "selection and acquisition of automatic data processing resources", May 19, 1972 (currently under revision), which establishes the policy that selection and acquisition of ADP resources must be based on well documented cost effectiveness studies. The third is DOD instruction 5010.27, "management of automatic data systems development," November 9, 1971. This instruction which is currently under revision establishes policies, procedures and responsibilities for the development of automated data systems. These three policy issuances implement OMB circular A-71, "responsibilities for the administration and management of automatic data processing activities," March 6, 1965, Federal management circular 74-5, "management, acquisition, and utilization of automatic data processing (ADP)," July 30, 1974, and General Services Administration Federal Property Management Regulations. The policy directives are supported by several DOD instructions addressing policy in specific areas such as ADP sharing and reutilization, data elements and data codes and ADP security. A synopsis of Department of Defense ADP policy issuances is contained in figure 8. Policy guidance is also issued in the form of economic guidance papers for those issues that require more elaboration (figure 9).

Within the military departments and Defense agencies, OSD policy is implemented in the form of departmental and agency instructions and regulations. For example, within the Army, the Directorate of Management Information Systems is the specific office that implements DOD policy in Army regulations (AR). Figure 10 contains a synopsis of the Department of Army ADP regulations. Similarly, the Information Systems Division of the Navy is the office that implements DOD policy via SECNAV and OPNAV instructions. A synopsis of Navy and Marine Corps ADP policies appear in figure 11. The Air Force Directorate for Data Automation issues implementing DOD policy in the form of Air Force regulations (AFR). Figure 12 contains a synopsis of Air Force regulations. Within the Defense Supply Agency (figure 13) implementing instructions and regulations are promulgated by the assistant director for plans, programs and systems.

As mentioned previously, various functional organizations publish supplementary guidance that impacts the ADP area. A selected list of such guidance appears in figure 14.

Your interest in the specifics of computer operations and related policies within the DOD components will be addressed in terms of the classification of computers, their number and dollar costs for general purpose computer operations, and the degree of reliance of the military departments on computers.

Computers are classified by the General Services Administration (GSA) as follows:

(1) General purpose computers which are commercially available and used primarily in general management and administrative applications.

(2) Special purpose computers which are used in unique operational environments such as command and control, and intelligence. They are also embedded in special configurations such as missiles, planes, ships, and land vehicles.

Based on the above classification, the inventory for fiscal year 1975 showed that DOD computers numbered 3,655, including 2,178 general purpose and 1,477 special purpose computers. The overall cost of general purpose computer operations for DOD in fiscal year 1975 was approximately $1.6 billion, including personnel costs. Comparable figures for 1959 show an inventory of 280 general purpose computers and a budget of $159 million. The program has now leveled off as indicated by a fiscal year 1972 inventory of 3,600 computers and a budget of $1.5 billion.

I will now discuss the nature and extent of DOD reliance on computers.

First, the DOD requires computers for such applications as personnel and logistic management, installation and inventory control, military and civilian pay, contractor and supplier payments, and maintenance scheduling, among others, in order to assure efficient and economical management or administration. This category constitutes by far the largest concentration of ADP resources in DOD.

Second, command and control and intelligence functions require computer support with the attendant requirements for real time, large storage, semiautomated response, random access, and high reliability. Such computers are critical to the DOD mission.

Third, computers continue to be essential in research, development, and test instrumentation and computation.

To best support what I understand to be the intent of your interest, I will concentrate on those applications identified in the first group. The loss of computer support in these areas can have numerous and far reaching consequences. Examples include the making of poor management decisions, jeopardized career advancement, delayed personnel pay, delayed payments to contractors and suppliers, loss of financial accounting, and the furnishing of inadequate information to other Government agencies and the Congress.

You expressed an interest in the use of computers in the disbursement or scheduling of payments or maintenance, and the actions initiated in an automated fashion commonly known as "automated decisionmaking." OMB, in a follow on to the GAO report, "Improvements Needed In Managing Automated Decisionmaking by Computers Throughout the Federal Government," initiated by your committee, is requiring Federal agencies to assess the extent of automated decisionmaking. DOD is responding to OMB's requirement and is taking the following actions:

We are reviewing all computer operations to determine the extent to which they involve automated decisionmaking applications.

In this connection we are reviewing existing policies, responsibilities, and procedures relative to the design, development, test, evaluation and approval of automated processes and systems, and all administrative procedures, criteria, computer programs, and so forth, pertaining to automated decisionmaking applications. The purpose is to assess the possibility and probability of improper actions, the extent to which any improper actions have or may be occurring and the impact of improper actions.

The results of these reviews will be evaluated, documented, and include corrective steps taken, underway or planned.

The results of these reviews will be included as a part of the narrative in the fiscal year 1978 ADP Budget exhibit submitted to OMB in late 1976. As a related topic, an immediate response to your question regarding the use of computers in the disbursement of payments in DOD is given below. Examples include in the disbursement of funds in two automated areas of personnel compensation and logistics.

On personnel compensation, the three military departments and the Defense Supply Agency (DSA) disbursed, with heavy reliance on computers, a total of nearly $30 billion annually. Of this total, it is estimated that $6.5 billion or over 20 percent were not subject to human intervention. In the logistics area, the military departments and DSA disbursed nearly $17.5 billion, of which it is estimated that $0.7 billion or 4 percent were not subject to human intervention. These figures are subject to change, of course, when the results of the extensive review I mentioned previously is completed.

As examples of our present efforts, an automated personnel compensation system and a logistics contract administration system using automated decisionmaking principles will be described. The systems do not provide for fully automatic decisionmaking by the computer. They have built in checkpoints, or controls, that signal to operators when an apparent exception occurs, for example, if a captain in the Army would be provided a total pay amount that exceeds the maximum that a captain could receive.

A representative example of an actual automated personnel compensation system in the Department of Defense is the U.S. Army's military pay system called the joint uniform military pay system—Army (JUMPS-Army). This is a centralized computerized pay system located at the U.S. Army Finance and Accounting Center, Fort Benjamin Harrison, Ind. All input data to the master military pay file of the military pay system is electronically transmitted from the local finance and accounting offices. Monthly, a computation cycle compiles an update of the master military pay file, prepares pay and allotment checks, composes listings, prints bonds, makes deductions, and withholds income and social security taxes. The central site makes minimal input to the master military pay file directly. The majority of the data is input from the field finance and accounting offices. After the monthly computation cycle is completed, payments in excess of $2,000 for end of month pay and $1,000 for midmonth pay are identified to the local finance and accounting offices for pay record audit for propriety of payments. Periodically, certain repetitive monthly entitlements; for example, quarters allowance, subsistence allowance, and so forth, are identified to local finance and accounting offices for reconciliation and certification. Monthly, a selected file comparison is made between military active accounts and personnel files to determine if authorized accounts are present in the military pay system. The Air Force also operates under a JUMPS pay system and the Navy will be operational under the JUMPS system by January 1977.

An example of an actual automated logistics system in the Department of Defense is the one known as "mechanization of contract administration services (MOCAS)" used in the Defense Supply Agency. This is a logistics system developed for the purpose of administering contracts. The system has the three classical types of controls; that is, separation of functions (organizational), internal controls, and audit trails. Formal and distinct separation of functions and human review of initial input characterize the system.

Thereafter, the MOCAS system assists in performing necessary contract administration functions such as meeting delivery schedules and disbursement of payments on the basis of programed decisionmaking criteria incorporated in computer instructions.

I understand that computer-related crimes is another central concern of your inquiry. DOD does not regard these crimes as being a separate category of offenses unto themselves. Many of the aspects of their investigation are pursued in the same manner as crimes not involving computers. For example, thefts of property ordered by a computer would still be investigated as thefts of property.

The fact that a computer was used would, however, require a number of additional leads to be pursued. Most of the investigative leads to be developed would be of a routine nature common to most cases but others might require either special computer knowledge or special computer techniques. These are acquired by DOD investigators through experience and training courses described later.

The DOD investigators coordinate and interface with other organizations both within their various departments as well as with other Federal, State, and local law enforcement, investigative, and judicial agencies. These contacts are also useful when computer-related crimes are involved. For instance, although the military investigative agencies do not have auditors assigned, audit assistance would be provided by audit agencies, should it be determined in an investigation that such services were needed. Hence, as the need requires there is a close working relationship between auditors and the investigators. An example in the civilian community is a pending computer-related investigation being monitored at the present time by the Air Force Office of Special Investigations. This case concerns the alleged theft of computer time, by a civilian, from a computer which is also being used by an Air Force facility. The theft was accomplished by "tapping in" to the system. Because such activity would require a terminal and the theft of such terminal equipment had been previously investigated by the Federal Bureau of Investigation, the entire matter was referred to the FBI.

Our investigators have been and are receiving computer oriented and specialized training. They have attended computer orientation courses developed and given by the Department of Defense Computer Institute (DODCI). These courses include an overview of security problems associated with using ADP system, such as remote access leakage possibilities, and administrative and management control procedures used in such systems.

In March 1976, the Air Force Office of Special Investigations (OSI) revised the curriculum of their specialized fraud investigation course to expand the instruction on computer technology and computer fraud. The current course curriculum includes 16 hours of instruction and a 3-hour practical problem. The majority of the instruction is provided by the staff of the DODCI. To date 47 OSI investigators and 14 from other DOD agencies for a total of 61 investigators have attended the specialized fraud investigation course.

The computer training currently being provided to OSI special agents raises their level of knowledge and their expertise in this area. It better equips them to respond to requests from investigations involving computer crime. Present academic treatment of computer abuse/security problems is not, however, sufficient for investigators to identify computer frauds or to be the persons responsible for initiating or recommending technical methods to increase the security of computer operations. Such a responsibility should rest more suitably with the technical experts in the data automation field. The main thrust of investigators is in the area of detection through human resources. Having special agents trained to respond to allegations of computer crime and to conduct professional investigations is a major objective of the training program and ultimately leads to deterrence. Within those limits, the level of instruction on computer abuse is sufficient to meet OSI's investigative mission responsibilities.

The U.S. Army Criminal Investigation Command (USACIC) is continuing to evaluate the potential for criminality through the use of Army computers and recognizes that special training is required for the detection and investigation of complex computer crimes, especially in the fraud area. The extent and the precise type of training required are being studied to insure that the degree of training equates to the need. It is anticipated that USACIDC agents will attend selected courses which will provide them with the additional technical expertise needed to investigate complex computer crimes. Some of the courses which can provide this expertise are currently in existence and will be modified to meet USACIDC requirements. Due to the dynamic and changing nature of ADP, courses will be periodically evaluated to insure that agents receive the proper amount of training.

Basic orientation in computers is also given at the Criminal Investigators Logistics Management Orientation Course (CILMOC), Fort Lee, Va. This 4-hour overview is designed to assist students in identifying computer abuse and fraud. To date, nearly 575 special agents and supervisors of the Army Criminal Investigation Command (CIDC); 75 OSI agents, 28 Navy IS agents, and 35 agents of the Defense Investigative Service have graduated. Of the approximate 4,000 special agents in the Department and its components about 740 or 19 percent have been given this training.

The 4-hour overview is an interim measure which, supplemented by knowledge obtained by agents from other sources, has been adequate to enable the agents to complete successfully the limited number of cases which have been identified. Nevertheless, the Department of Defense investigative agencies are keenly aware of the potential for computer-related crimes or abuses and are taking and planning actions designed to upgrade their ability to detect and investigate such crimes.

Within the Department of the Army CIDC 16 investigations have been identified through coordination with CIDC field elements and review of available records at the headquarters. Of the 16 cases identified, 15 involved the manipulation or alteration of input to obtain a favorable result for the perpetrator. These 15 investigations ranged from submitting fraudulent requisitions into the logistics supply system in order to obtain items for wrongful disposition to a scheme by two enlisted personnel to submit fraudulent input to finance computers in order to obtain duplicate pay. In two instances, computer rejection of bogus input foiled the successful perpetration of the crime. The one remaining investigation of the 16 examined involved allegations of conflict of interest on the part of computer management personnel. While major crime was not determined in this particular investigation an extensive crime survey was written detailing management problem area. The investigation and survey resulted in corrective action being taken by the Department of Army element involved.

The Naval Investigative Service identified the following cases:

(1) An investigation was conducted to resolve allegations that an individual could use free computer time and obtain encrypted information from military computers by manipulation of computers at a nearby university. The allegations were disproven.

(2) An investigation was conducted into the attempted fraudulent procurement of parts valued at $84,800 which had been requisitioned by introducing false documentation into the supply network computer system. The attempt was detected and the Government did not sustain a loss. Two foreign national suspects were identified and reported to local authorities.

(3) Another instance of false computer documentation being submitted for processing occurred at a major overseas military base supply center causing tools and replacement parts valued at $5,600 to be fraudulently requisitioned. Although no suspects were identified most of the merchandise was recovered.

(4) An investigation is currently underway to resolve allegations that after two former officers and one civilian employee terminated their Government service, they misappropriated a Government "software" package, formed a commercial firm, and subsequently won a contract to provide both computer hardware and the misappropriated "software" package to the Government agency for which they formerly worked.

The Air Force Office of Special Investigations identified 16 investigations to the GAO in 1974 as being computer related. Of these 16 cases, only 13 actually involved a computer as an instrument of the crime. Computers were not involved in the other three cases. All of the 13 involved the manipulation or alteration of input to obtain a favorable result for the perpetrator. Three of these investigations involved attempted financial gain by either entering false requisitions into the logistic supply system to obtain items for wrongful disposition or to manipulate stock accounts. Three investigations were concerned with the manipulation of leave time and another four involved altering, deleting, or filing efficiency reports. Two investigations concerned manipulation of a computer for preferred assignments and the final investigation concerned a false computer entry which allowed ineligible individual to reenlist. In two of the investigations the computer itself rejected the entries.

In 1974, AFOSI and FBI investigations discovered and prevented the fraudulent shipment of U.S. Government property valued at $830,000. This investigation was pursued and further disclosed that fraudulent diversion of U.S. Air Force communications equipment through computer manipulation had occurred during 1972–74. A review of computer transactions revealed that shipments of 145 items, valued at nearly $575,000 had been diverted from the Air Force and sold to unknown commercial sources. An additional 45 items, valued at nearly $333,000 had been shipped but were subsequently recovered by military authorities and the FBI. The individuals responsible for these incidents were apprehended and prosecuted.

From the information available to the Department of Defense, several general conclusions regarding computer-related crimes relative to the DOD can be stated:

> (1) Computer input can be manipulated by knowledgeable persons with access to the computer in such a way that crimes can be committed in the same way a bookkeeper can manipulate entries in the ledgers of a business.
>
> (2) While computers in themselves do not necessarily make it any easier to commit a crime, such crimes may be harder to detect.
>
> (3) In most cases, internal stops or controls can be built into a computer to detect inappropriate or erroneous input, as demonstrated by several of the examples cited. The critical factor is whether the functional manager has adequate controls built into the functional system specifications.
>
> (4) Unscrupulous persons having special expertise, special equipment, and access information can carry out a criminal act with a relatively high degree of success. The critical factor is the amount of resources available to meet the threat.

The cases identified thus far indicate that the majority of the crimes were committed by personnel with relatively limited knowledge of computer technology. The possibility does exist that more knowledgeable personnel as well as any other personnel might be involved in computer fraud. Our knowledge is limited to those cases which have been reported and these are not necessarily indicative of the total crime picture. Although the possibility of senior level involvement exists the probability has not been established. Because senior personnel may or may not have a more advanced knowledge of systems and component vulnerabilities it does not necessarily follow that this knowledge can be translated into the ability to commit a crime and avoid detection. Senior personnel do have an overview because of their management role. However, it would appear that those who are involved in computer operations on a day-to-day basis have the best opportunity to take advantage of the technical knowledge they possess. As indicated in the previously mentioned cases, a large percentage of the crimes consisted of falsification of input documents. These crimes for the most part were committed by clerical personnel. In our opinion, these types of crime can be minimized by building more audit controls into the computer software. In this respect, a draft DOD instruction is presently in coordination that will require among other things that internal auditors be involved in the design phase of ADP systems development. The intent is to insure that appropriate controls are built in at the front end and minimize the need to retrofit operational systems with audit controls. This is another means to insure system integrity.

DOD Directive 7600.3, "Internal Audit in the Department of Defense," issued by the Assistant Secretary of Defense (Comptroller) assigns the DOD audit policy, coordination, and evaluation functions to the Deputy Assistant Secretary of Defense (Audit), and identifies the responsibilities for various audit operations to him and the centralized audit organizations in the military services and the Defense Supply Agency.

Figure 15 presents the placement of audit organizations in the Department of Defense as of December 1, 1976.

DOD audit policies and procedures are consistent with the audit policies prescribed by GSA Financial Management Circular 73-2, "Audit of Federal Operations and Programs by Executive Branch Agencies," and the "Standards for Audit of Governmental Organizations, Programs, Activities, and Functions" issued by the Comptroller General of the United States.

The internal audit organizations are centralized and independent of the operations they review. Therefore, objective appraisals can be made of the efficiency and effectiveness in which managerial responsibilities are being carried out at all levels throughout the Department of Defense.

Internal audits are directed toward determining that management controls, practices, and procedures are adequate in concept and effective in application and that they provide for adequate financial integrity and effective utilization of available resources. Internal audit provides an essential managerial control which measures and evaluates the adequacy of systems, procedures, and internal controls. Through audit, appropriate recommendations are developed regarding conditions that cause or contribute to inadequate controls or inefficient, or uneconomical operations. DOD audit policies concerning the study and evaluation of internal controls are consistent with the basic audit concepts and standards prescribed by the American Institute of Certified Public Accountants (AICPA).

To achieve maximum audit effectiveness, the DOD internal audit agencies require highly competent audit staffs. The DOD audit policies in this regard require the internal audit agencies to establish recruiting, training, and career development programs necessary to develop and maintain a competent and effective professional staff. The programs and professional staff qualifications of each internal audit organization must conform to the prescribed standards established by DOD.

DOD audit policies relative to staff qualifications are in full compliance with the AICPA's first general auditing standard which states that "the examination is to be performed by a person or persons having adequate technical training and proficiency as an auditor." If a DOD component undergoing audit has or is supported by an ADP system, the auditors need to understand the ADP system sufficiently to enable them to identify and evaluate among other things its essential security control features.

As of June 30, 1976, the total combined personnel strength of the five DOD internal audit organizations was 2,679. Of the 2,264 professional auditors and technicians included in that total, 1,858 or about 82 percent had ADP and ADP audit training and experience (figure 16).

The larger DOD internal audit organizations have developed and conducted their own programs to provide basic training in skills such as ADP systems orientation, COBOL programing, ADP auditing, and computer assisted audit techniques. In addition, a number of other educational facilities, within and outside the Defense Department, are utilized to obtain a wide range of ADP technical knowledge for DOD internal auditors. A partial list of the other ADP training programs appears at figure 17. In the 24-month period comprising fiscal years 1975 and 1976, DOD internal auditors received about 10,000 man-days of formal training in ADP and ADP audit techniques in addition to the informal on-the-job ADP training provided during audits.

All of the DOD audit organizations have computer assisted audit techniques available to use in the audits. These techniques involve the development of audit routines in computer program form so the ADP system can be used to audit data processed or contained in the computerized records. Some examples of computer assisted audit techniques being used within DOD are as follows:

The Air Force Audit/Management System (AFA/MS), an audit retrieval package developed by Arthur Young & Co., certified public accountants, was one of three information retrieval packages used by the Air Force Audit Agency.

The Army Uniform Data Inquiry Technique (Audit), the audit retrieval software package developed by the Army Audit Agency is used extensively by Army and Defense Supply Agency auditors.

Naval audit service auditors use CARS II, the computer audit retrieval system developed by Computer Audit Systems, Inc. Although these computer audit routines differ in several respects, all of them are designed to use the computer as an audit tool in extracting and comparing data and in making mathematical calculations; and all have the program capability to apply statistical sampling methods in audit tests.

In addition to the specialized computer audit routines developed primarily for auditors, the DOD audit organizations subscribed or had access to computer timesharing services. These services provide access to standardized software programs dealing with probability and statistics, population statistics, regression analysis, analysis of variances, time series analysis, distribution functions, data comparison, control charts, sampling plan evaluation, system simulators, plotters and histograms, etc.

During the 24-month period comprising fiscal years 1975 and 1976, the DOD audit organizations issued 66 reports on audits and studies of ADP systems development projects. Thirty-five of these reports covered various aspects of ADP systems undergoing development, 12 reports covered audits performed during the system prototype of test phase and 27 related to ADP centers. The reports dealt with matters such as system requirements, lease versus purchase decisions, organization and operations controls, documentation, system management, hardware/software configuration controls, access to facilities and files, and application (including input, processing and output) controls.

Besides auditing developmental systems, internal audit organizations issued 178 reports with one or more findings relating to operational ADP systems. There are two reasons for the large number or reports in this category. First, due to the nature and volume of transactions, most DOD organizations, programs, activities, and functions have or are supported by ADP systems. Secondly, the application of generally accepted audit procedures usually discloses existing deficiency conditions in internal controls in supporting ADP systems. For example, the conditions described in several findings in the DOD audit reports cited in the GAO report entitled "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government," April 23, 1976, were identified by DOD internal auditors in their examinations at DOD components supported by operational ADP systems, rather than in audits limited to the ADP system hardware, software and facilities.

As a result of the DOD internal audit coverage of ADP systems provided by the 244 audits, over 400 findings with recommendations to improve the efficiency, effectiveness and economy of ADP systems or to correct weaknesses in system internal controls were made to DOD operating officials. These recommendations were approved and have been implemented in many areas.

Each DOD organization has established procedural guidelines for auditors to follow when potentially fraudulent or unlawful activities are disclosed during their examinations. Generally, these guidelines require that the circumstances of the suspected illegal practice be reported confidentially, but immediately, to audit agency headquarters and to other appropriate DOD officials and investigators. Pending specific instructions, the auditors are normally expected to continue their examination in accordance with the original audit place, exercising caution and good judgment so as not to reveal their suspicions to other personnel or impair subsequent investigations in any way.

During the 2-year period ending June 30, 1976, a number of instances of potential fraud, theft, and criminal activities were disclosed during DOD audits. None of these instances involved the use of computers or could be characterized as computer-related crimes. A logical question at this point is "Are our audit procedures adequate from a technical standpoint?"

On June 2, 1976, the Deputy Assistant Secretary of Defense (Audit) directed his internal audit policy staff to make a study of "ADP Systems Evaluations by DOD Internal Audit Organizations." The study will enable the DASD (Audit) to assess the adequacy of the present level of efforts, skills, and training in ADP system technology and audits. Technical skills and special training requirements for participating auditors will be reexamined. The purpose of the study is to recommend any desirable changes in ADP audit techniques, coverage, training, and staffing.

In addition to continuing to apply a large portion of their audit resources individually to examinations of ADP systems undergoing development, undergoing prototype testing, and currently operational, the DOD internal audit organizations have initiated two DOD-wide audits which are being jointly researched, planned, and performed under the direction of project managers in the Office of the Deputy Assistant Secretary of Defense (Audit). They are:

(1) The interservice audit of DOD accounting systems requiring the approval of the Comptroller General of the United States; and

(2) The interservice audit of systems security and data privacy at DOD data processing installations.

I would like to turn now to computer security. The GAO report entitled "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities," dated May 10, 1976, states that ADP security procedures are inadequate in several Federal agencies.

As indicated in our response to the GAO, we generally agree with this finding. In our opinion, the history associated with ADP security is extremely important in providing us with the necessary basis upon which to establish future initiatives. In this respect, the GAO report serves as an excellent reference.

Current DOD policies address many of the problem areas outlined in the GAO report. Moreover, DOD is continuing to participate actively in the task group of the National Bureau of Standards addressing the computer security problem. In particular, DOD provided its Directive 5200.28, "Security Requirements for ADP Systems" and its accompanying manual to the NBS as input during the development of FIPS PUB 31, "Guidelines for Automatic Data Processing Physical Security and Risk Management." In our opinion, the DOD policies and NBS guidelines together form an excellent basis upon which we can further strengthen our ADP security posture to protect against vulnerabilities such as natural disaster, unauthorized access, unauthorized alteration of data, and unauthorized use of data and equipment.

Enforcement of ADP security policies within the Department of Defense consist of procedures such as internal audits, ADP system reviews by management review teams, and the designation of ADP security officers at data processing installations. For example, the Computer Security Division of the U.S. Army Intelligence Agency has a staff of counterintelligence and ADP specialists who perform reviews of selected data processing installations (DPI's) for ADP security. This organization has two operational branches. The first consists of three similarly configured teams and conducts ADP systems security evaluations of designated DPI's. The second, the Analysis Branch, is responsible for maintaining an awareness of the state-of-the-art in ADP and security technology as it affects the security of ADP systems. Additionally, continued update training in an individual's primary specialty is required to attain and maintain an indepth technical knowledge of state-of-the-art advances in the fields of counterintelligence and automatic data processing.

The DOD also places a strong emphasis on backup systems and contingency planning. This is done not only through the establishment of appropriate policy but also through the periodic testing and evaluation of such plans. For example, the Defense Supply Agency has a computerized personnel system located at Cameron Station with three alternate sites for emergency planning purposes. To insure confidence in their continuity of operations plans, testing was performed at all three sites. Test results indicated that the personnel system processed satisfactorily at each alternate site. There is currently a draft DOD instruction in coordination titled "ADP Systems Life Cycle Management" which calls for the development of an ADP system master plan for each major ADP system. This master plan includes the development of a plan for continuity of operations. Publication of this DOD instruction is expected some time in fall 1976.

With regard to the securing of military computer systems, you asked the Department's response to the assertion by many computer experts that, given adequate resources, a violator can compromise any computer system he sets out to compromise. Here, the key word, and variable, is "adequate." In all of our security programs, we must assume that given "adequate" resources, a penetrator can compromise any target, including a computer system, which we wish to protect. What all of our security programs do is attempt to make such penetrations prohibitively difficult in terms of cost, returns, and risk to the penetrator. The penetrator, of course, does not have unlimited resources. Neither do we in defending against him. Our approach is to allocate the preponderance of security dollars to the protection of the most sensitive material. That, in fact, is the significance of categorizing national security information and material on the basis of relative sensitivity and compromise impact for the purpose of allocating security expenditures.

Unclassified data in an ADP environment is inherently more protected than in a non-ADP environment. This added protection is a result of several factors. To begin with, almost all of such data is resident on machine readable storage media such as magnetic tape or disk. Access to such information thus requires execution of a program to output the data to human readable format. This in turn requires gaining access to the computer, either onsite or through a remote terminal, and knowing and employing existing access controls or in some manner circumventing such controls. Such controls are stricter and more rigidly enforced in an environment where classified data is processed.

The Department of Defense has recognized the vulnerability of computers for quite some time. Currently, the majority of our policies and procedures focus on the protection of classified information which was the area of our earliest efforts.

The specific question of adequate protection of classified information stored or processed in remotely accessed resource sharing computer systems was first formally surfaced in the Office of the Secretary of Defense in April 1967. This was followed that same year by the formation of a task force on computer system security under the Defense Science Board, composed of experts on the subject from Government, industry, and the academic community. Their report, finalized in early 1970, was the first attempt to codify the principles and details of this very involved technical-administrative problem.

This report served as invaluable input to the Department of Defense ADP Security Task Force, formed in February 1970 to develop necessary security policy directives utilizing the advanced technology in automatic data processing systems. The products of this task force were Department of Defense Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems", dated December 18, 1972, and its companion "DOD ADP Security Manual, 5200.28M" of January 1973. These documents establish uniform Department of Defense policy for the development, use, and evaluation of techniques and procedures for the protection of classified data stored, processed, or used in, and classified information communicated, displayed, or disseminated by, an automatic data processing system. Concurrently, Defense was among the first, if not the first, to establish formal training for ADP system users, computer specialists, and security specialists who will be engaged in the development, management, and operation of secure ADP systems. In this regard, initial DOD Computer Institute pilot courses were conducted as early as 1969, with other ADP security training courses relating to the requirements of the directive having been in existence on a continuing basis since 1972. These courses served to provide a partial solution to one of the crucial problems in DOD's ADP program, that is a shortage of multidisciplinary trained manpower dedicated to the automation security mission.

In 1975, a related course on computers and privacy was established by the Institute. Over the past 2 years, 2,862 personnel have participated in these courses.

Given that the hardware and software of most currently available computer systems is not fully secure and that securing computerized systems poses a unique and complex kind of security problem, the Department of Defense requires the testing, evaluation, and approval of each ADP system handling classified information and specifically assigns responsibilities toward that end.

Contractors requiring access to or possession of classified information in connection with the performance of a contract must execute a DOD Security Agreement (DD form 441) with the Department of Defense. Such contractors are required to follow the uniform security practices established by the Department of Defense Industrial Security Manual for Safeguarding Classified Information. Before a contractor is eligible for access to classified information, a facility security clearance is required. This is a determination as to the eligibility of the facility from a security viewpoint for access to classified information of the same or lower classification category as the clearance being granted. Contractor employees whose access to classified information is essential in the performance of a contract as well as certain other individuals (Chairman of the Board and all principal officers, directors, and other appropriate executive personnel) require security clearances. Further, before a contractor is eligible for custody of classified information he shall have storage capabilities for classified information and be prepared to apply the safeguards prescribed by the DOD Industrial Security Manual.

Recurring security inspections are conducted for all previously cleared contractor facilities having access to classified information. These DOD inspections insure that the procedures, methods, and physical safeguards prescribed in the DOD Industrial Security Manual are employed by contractors for the protection of classified information entrusted to them. These inspections are normally conducted by DOD personnel under the Executive Directorate, Industrial Security, Defense Supply Agency. Inspection scheduling is normally based upon the highest level of classified material possessed at the facility since the preceeding inspection, and the frequency ranges from 6 months in the case of top secret and secret to 9 months for confidential.

A special section of the industrial security manual specifies conditions and prescribes security requirements under which ADP systems will be operated when handling classified material. The section provides for the application of administrative, physical, and personnel security measures required to protect classified material processed or resident in ADP systems from inadvertent or deliberate compromise. As a general rule, all persons who operate or access an ADP system that stores or processes classified information must have a security clearance for the highest classification and most restrictive category of classified material contained or processed in the ADP system.

One methodology which has been employed to evaluate the level of security in a system is that of the so-called Tiger Team or Penetration Team approach. The essence of a Tiger Team is a group of knowledgeable and competent computer scientists, particularly in the operating systems programing area, who attack the hardware and software security measures of a system. Although the level of effort has varied, computer system security tests undertaken within DOD have tended to reveal some soft spots, or vulnerabilities, in the hardware/software security area. When given direct access to a computer system, Tiger Teams can, with a relatively low level of effort, penetrate the minimal security controls available on current commercially available computer systems. This stems from the fact that the overwhelming majority of the operating systems now commercially available were not designed with security as a rigorous or high priority design goal. At the time such systems were being designed, user requirements emphasized resource sharing to maximize processing throughout. The security features which exist in such operating systems were designed to allow multiple concurrent processes to exist without program or data interference. These features were either automatically invoked or provided as the result of the user following predefined procedures. The design assumed that the users wanted to avoid interference and would abide by the procedures. Time sharing service bureaus identified the inadequacy of such security controls and tailored these operating systems to provide needed measures that their customers demanded.

Development of secure operating systems has been underway for several years. The problem is acknowledged as difficult and centers on designing a software module that exercises absolute control over all user accesses; allocation of resources, programs and data; and then certifying that this software module has no design or programing flaws. Until these problems are resolved we are limited to a Tiger Team approach.

The recent Naval Research Laboratory (NRL) test and evaluation of a UNIVAC computer system is an example the Tiger Team approach as well as a specific example of our policy in action. Since there has been quite a bit of misunderstanding concerning this effort, I wish to make several brief points:

> The test was formally requested through channels pursuant to the Navy's implementation of DOD directive 5200.28 "Security Requirements for Automatic Data Processing (ADP) Systems" and DOD manual 5200.28M "Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems."
>
> The NRL personnel conducting the test were accordingly properly cleared, had valid security visit requests to the facility operating the UNIVAC 1108 computer system, had additionally been granted formal access to the computer system as such, and conducted their tests of the system via a terminal directly connected to the system within its protected facility. That is, NRL personnel were given direct access to the system and its facility, permitting them to bypass the system and facility safeguards that normal outsiders would have to overcome.
>
> Further, the classified material removed from the UNIVAC 1108 computer system during the NRL test was handled by personnel having the proper security clearances and was given proper protection throughout the test.
>
> The test site, upon becoming aware of the vulnerability, immediately instituted a temporary administrative solution (prohibiting utilization of any reentrant processor). The final hardware/software modification (optimum memory protection feature), eliminating the weakness exploited by NRL and replacing the earlier interim administrative control procedure, has been implemented at the site.
>
> Additionally, the NRL Memorandum Report (No. 2821), published in June 1974, was distributed to all Government users of UNIVAC 1108 computers.

However, as I noted before, the UNIVAC 1108 EXEC-VIII operating system, like other vendor's similar commercially available operating systems, is large and complex (about 500,000 lines of computer program coding). Indeed, the NRL report described the exploited flaw as one of a class of problems likely to be found in any modern operating system. The NRL effort was only part of a comprehensive examination of the UNIVAC 1108 system, and that overall effort is not yet completed.

You requested cooperation in reprinting the report of the NRL penetration, and neither we nor the Department of the Navy interposes any objection.* You also requested assistance in preparing an easy-to-understand summary of the penetration exercise, and a Navy submission toward that end is appended at figure 18 for your consideration.

Besides identifying security problems with current commercially available computer systems, another major outcome of our vulnerability testing program has been to point up the difficulty and expense which would be incurred in making quantum security improvements in these systems. Sophisticated software security computer program enhancements or retrofits added to such systems do not tend to gain an amount of additional security consistent with the effort because the basic operating systems furnished with the hardware, which control all system resources, are themselves vulnerable to penetration. Correcting these operating systems is not an easy task; it must be remembered that current operating systems consist of a large number of complicated programs interacting in very complex ways. For example, the UNIVAC 1108 operating system, discussed above, was developed by hundreds of individual programers. The cost of retrofitting a computer system for security when such was not originally designed is substantial. A British privacy study estimated some time ago the cost of a total security retrofit was five times the original designed-in security cost. In addition, retrofitting to overcome a known deficiency may have systemwide impact. Experience has shown that patching one hole may open several other holes leading to a succession of required modifications. Retrofit of a system or program has another significant drawback in that it only fixes known deficiencies. Retrofit in no way certifies a system or program as secure. In this regard an Air Force computer security technology planning study cited the cost of a large-scale, contemporary operating system being repaired after a previously successful penetration exercise. The repairs involved over 250 changes and took 10 to 15 man-years of effort over a 6-month period. A second penetration exercise against the repaired system was successful in less than one man-week of effort![5]

Estimated cost comparisions for the repair effort versus the penetration effort were developed by the Air Force Study and are depicted in figure 19.

Another consideration in "retrofitting" an operating system is that once a user modifies portions of the operating system code, the vendor who developed the system will no longer guarantee support for that system. This means that the user who modifies or tailors a system must maintain his own expertise and support for the system.

The solution to obtaining a certifiably secure operating system lies in including necessary controls in the initial system design. Success in this area is not anticipated for several years. In May of 1972 at the spring joint computer

---

*The NRL penetration report may be found in the appendix beginning on p. 278.

conference, the chairman of the board of IBM committed IBM to invest in the neighborhood of $40 million in a long-range program to strengthen data security research and technology. IBM's efforts have focused on enhancement of a specific operating system called virtual machine (VM-370). IBM has corrected all known deficiencies in VM-370 and is committed to fixing any deficiencies that are identified in the future. IBM has also announced a new program product called the resource access control facility (RACF). RACF is designed to extend the data security capabilities of VM-370 by exercising stricter controls over user access to online files.

Honeywell Information Systems recently submitted a proposal to develop a certifiably secure operating system with a price tag of $25-$30 million. This proposal is still under evaluation. From an operational standpoint there are some significant factors. Development of a specific secure operating system must be undertaken with a target suite of hardware. Once the operating system is certified as secure, it is only usable on a specific set of computers which would effectively eliminate competitive acquisition of computer hardware for secure systems. At this point in time, the Department supports the development of concepts and techniques that will promote the further development of secure operating systems for any suite of computer hardware.

Of course, identifying problems is one thing, but solving them is another. In DOD, we are approaching these problems on three broad fronts. There are short term improvements, longer term research and development, and top level management initiatives.

With respect to short term improvements, our policies in DOD directive 5200.28 provide for the application of administrative, physical, and personnel security measures required to protect ADP equipment and installations from inadvertent or deliberate compromise, theft, damage, or destruction. Further, classified material contained in an ADP system is safeguarded by the continuous employment of protective features in the system's administrative, physical, personnel, and communication security controls. Emphasis continues to be placed on the latter controls to compensate for deficiencies in the state-of-the-art hardware and software protective features.

This policy solution is not without cost. Some of these are direct costs. Such costs include purchasing computer systems to be "dedicated" to processing classified material and clearance costs for ADP system users who may not require access to classified information but will have access to the system. Other direct costs are physical security, communications security, and emanations security costs for all remote terminal areas, regardless of whether or not they are actually required to process classified information. Less tangible costs and constraints include users' inability to use a system for certain periods of time, less than optimum employment of computer resources and the overhead involved in changing the security level of a system.

To overcome these undesirable byproducts inherent in the short-term approaches, we have embarked on some longer term efforts which should be of interest to this committee. The aims of these efforts are to achieve secure operating systems and to develop and implement adequate hardware and software security standards. For example, we wish to achieve a solution to security problems inherent in processing different categories of classified information concurrently (multilevel processing). Multilevel processing cannot now be accomplished in a secure manner because the operating system software of computers now in use has been proven to be relatively insecure. In particular, we want to develop techniques to assist in measuring the technical security attributes of a system. This would permit comparative evaluation of different systems, the ability to measure progress and the ability to establish tradeoffs between hardware and software measures and conventional security measures in approaching an acceptably secure operational posture.

The requirements for secure operating systems and a related standard are reinforced by the following:

(*a*) Ever increasing utilization of and dependence upon ADP systems for mission accomplishment;

(*b*) Increased sharing of expanding systems (i.e., more information, functions, users, and remote terminals added to systems);

(*c*) Increased internetting of our systems; and

(*d*) The Privacy Act of 1974 which imposes security protection requirements on an additional set of computer-processed information. To meet these requirements, DOD is funding significant research and development projects. Current R. & D. examples, responsive to the technical problems outlined include a number of projects of the Defense Advanced Research Projects Agency (DARPA). Several of these projects are oriented to the development of secure operating systems and message switching systems.

In turn, the DOD R. & D. effort is complemented by continuing DOD interaction with other Government, industrial, and academic efforts. For example, DOD continues to be an active participant in National Bureau of Standards projects for ADP security improvement. In this regard, we have taken appropriate action to ensure that all levels of ADP management become familiar with the NBS "Guidelines for ADP Physical Security and Risk Management" (FIPS PUB 31).

Although DOD has focused on computer security for nearly a decade, perhaps the most significant indicator of top management's concern for computer security is the fact that "Improving ADP Security and Safeguarding Personal

Privacy" was established as an official Department of Defense automation objective by the Assistant Secretary of Defense (Comptroller). This was done with full support of each military department and Defense agency.

A specific action required by both the DOD automation objectives and DOD Directive 5200.28 is the establishment of a central capability. Its purpose would be to assist and advise the military departments and Defense agencies in ADP systems testing and evaluation and to assess progress toward development and installation of secure ADP systems. To carry out the intent of DOD Directive 5200.28, the requirement has been refined, and evolved into the establishment of an ADP Security Management Council composed of senior managers throughout DOD. The functions of this Council will include the articulation of overall security requirements, the identification of technological improvements in ADP security to meet these requirements and oversight of the implementations. Participation on the Council will also get the military departments more involved in ADP security.

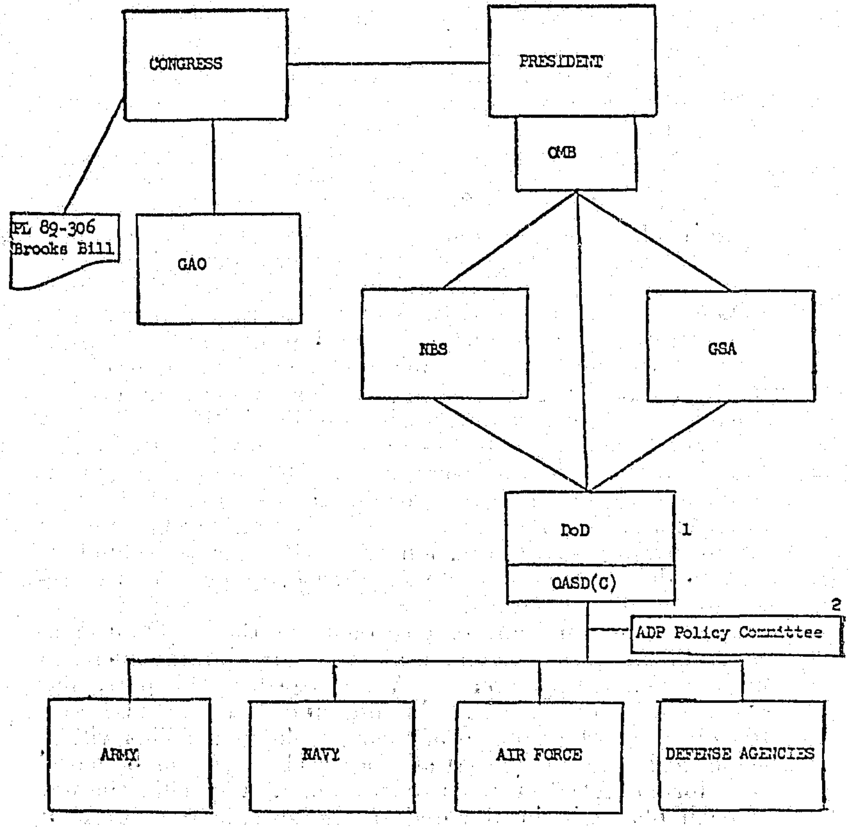
A small technical staff has recently been authorized under the Deputy Assistant Secretary of Defense (management systems) to coordinate the work of the multiple DOD areas of expertise. Two key functions of this staff will be to effect an interchange of information on ADP security technology and to design and promote ADP security programs in response to common needs.

Another action being taken to achieve the DOD automation objectives is the modernization and improvement of major defense ADP policies. A key aspect of this particular effort is to strengthen the planning and design of ADP systems in the earliest stages of their development. This will be achieved by requiring that all major ADP systems be based on a formal ADP systems master plan. A specific chapter of each plan will be devoted to the specification of ADP security requirements.

To summarize, Mr. Chairman, the rapid growth and sophistication of ADP has brought with it many benefits for economy and effectiveness. In taking advantage of these benefits, the operations of the Department of Defense have been changed in fundamental ways. Overwhelmingly, I think this change has been for the better, but there have been and will continue to be problems. For these reasons the Department of Defense has since 1967 continued to emphasize the management and technical control measures which I have been discussing. It is also the reason for our desire to work with you and the members and staff of this committee in this review.

FIGURE 1

DoD ADP MANAGEMENT PROGRAM



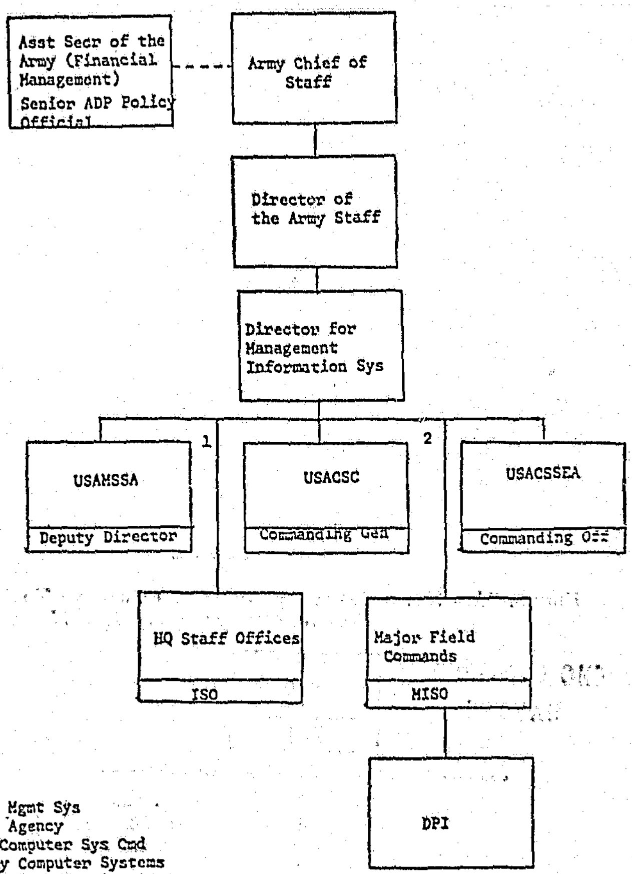
1/ Responsibility for the management of computer operations resides within the Office of the Deputy Assistant Secretary of Defense for Management Systems.

2/ Composed of DoD Component Senior ADP Policy Officials and chaired by the Deputy Assistant Secretary of Defense for Management Systems.

———— Command Line
------------ Principal Communications Channel

FIGURE 2

DEPARTMENT OF THE ARMY ADP PROGRAM


Asst Secr of the Army (Financial Management)
Senior ADP Policy Official
Army Chief of Staff
Director of the Army Staff
Director for Management Information Sys
1
2
USAMSSA
Deputy Director
USACSC
Commanding Gen
USACSSEA
Commanding Off
HQ Staff Offices
ISO
Major Field Commands
MISO
DPI

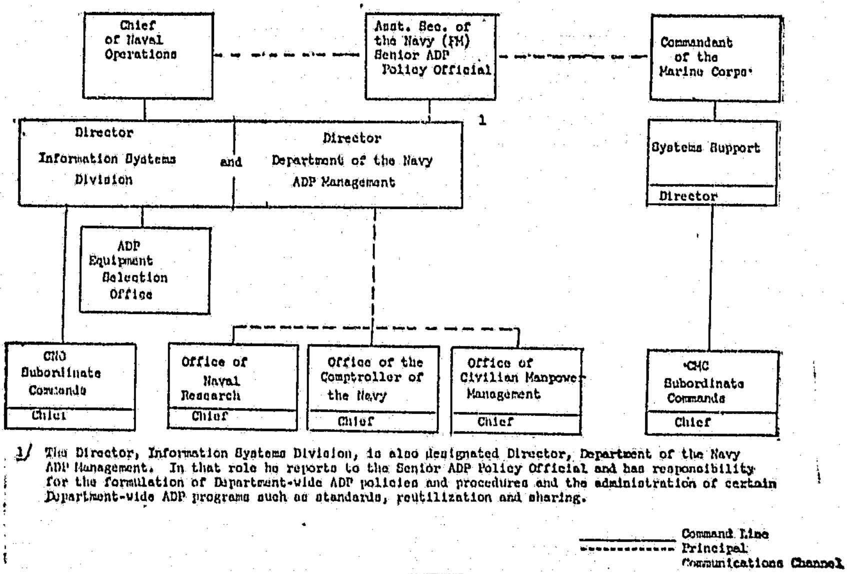
1. USAMSSA – US Army Mgmt Sys Support Agency
2. USACSC – US Army Computer Sys Cmd
3. USACSSEA – US Army Computer Systems Support & Evaluation Agency

———————— Command Line

- - - - - - - - Principal Commo Channel

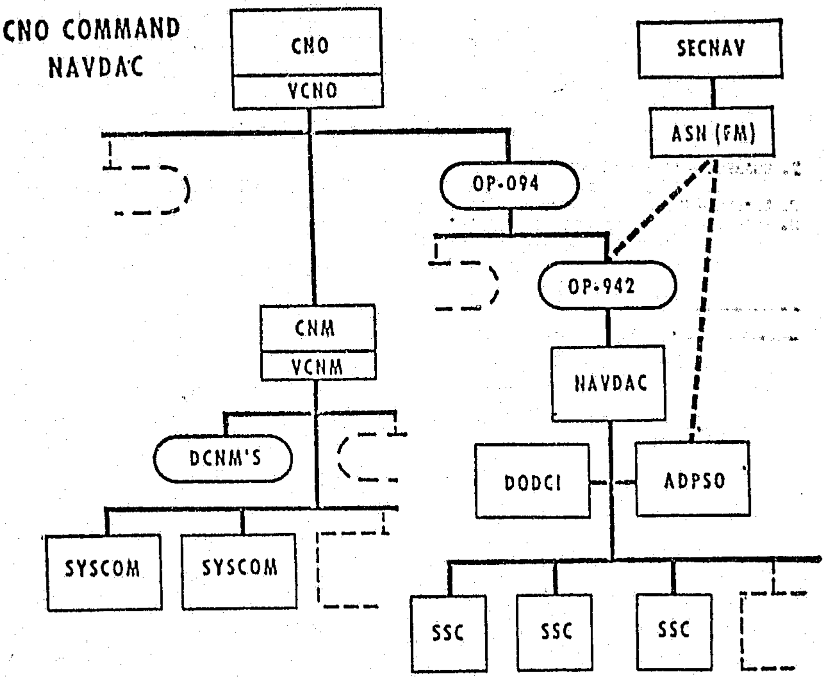
FIGURE 3

DEPARTMENT OF THE NAVY ADP PROGRAM


Chief of Naval Operations
Asst. Sec. of the Navy (FM) Senior ADP Policy Official
Commandant of the Marine Corps
1
Director Information Systems Division
and
Director Department of the Navy ADP Management
Systems Support
Director
ADP Equipment Selection Office
CNO Subordinate Commands
Chief
Office of Naval Research
Chief
Office of the Comptroller of the Navy
Chief
Office of Civilian Manpowe Management
Chief
CMC Subordinate Commands
Chief
Command Line
Principal Communications Channel

1/ The Director, Information Systems Division, is also designated Director, Department of the Navy ADP Management. In that role he reports to the Senior ADP Policy Official and has responsibility for the formulation of Department-wide ADP policies and procedures and the administration of certain Department-wide ADP programs such as standards, reutilization and sharing.

FIGURE 3A.—NAVAL DATA AUTOMATION COMMAND TO BE IMPLEMENTED COMMENCING JANUARY 1, 1977



Naval Data Automation Command to be implemented commencing 1 January 1977.

FIGURE 4

DEPARTMENT OF THE AIR FORCE ADP PROGRAM

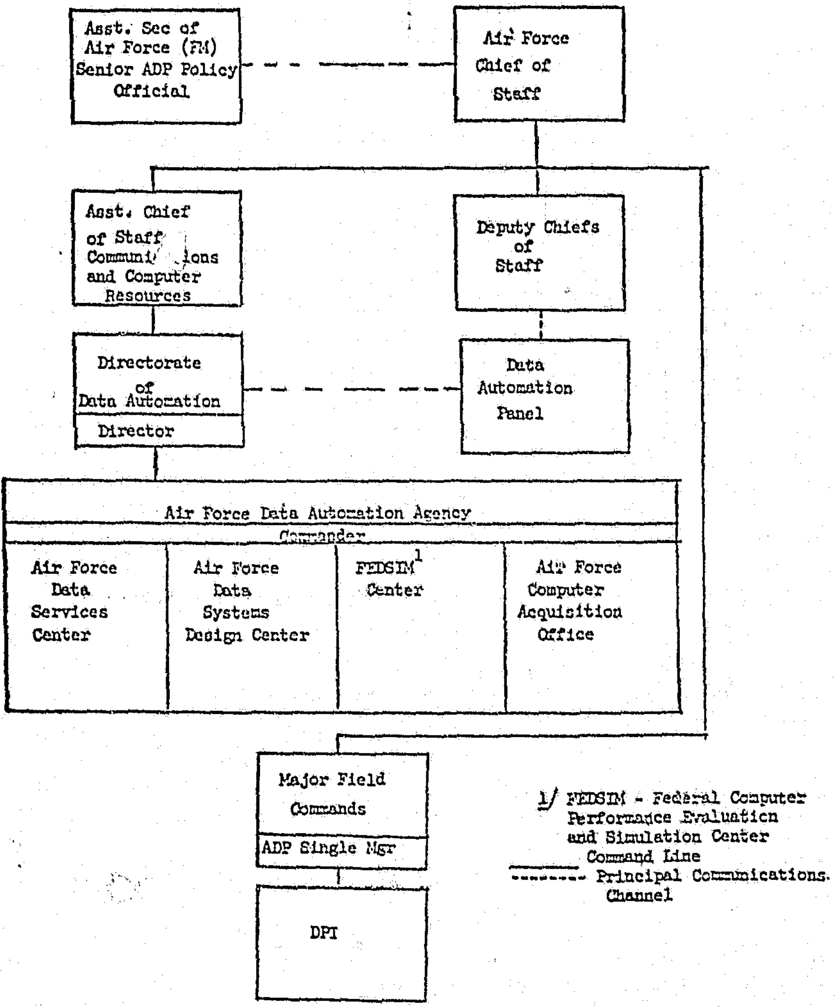
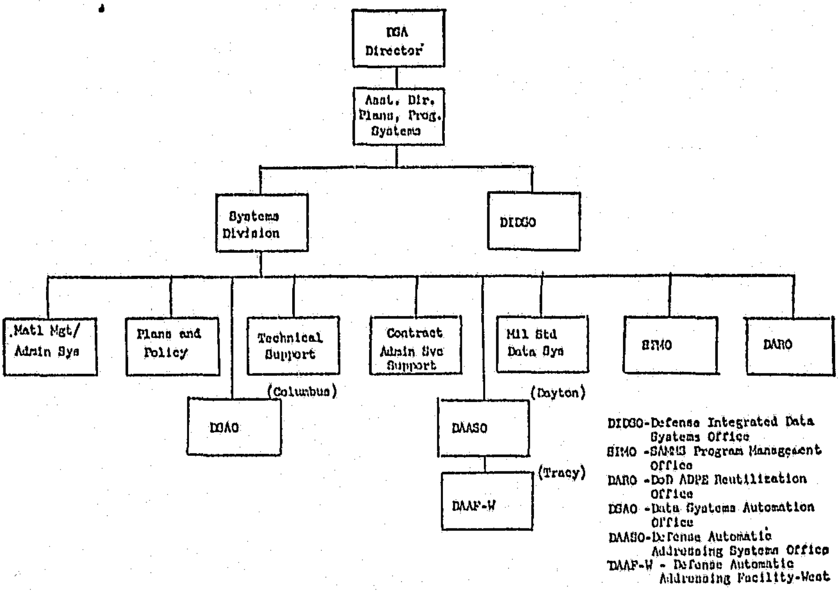

Asst. Sec of Air Force (FM) Senior ADP Policy Official
Air Force Chief of Staff
Asst. Chief of Staff Communications and Computer Resources
Deputy Chiefs of Staff
Directorate of Data Automation
Director
Data Automation Panel
Air Force Data Automation Agency
Commander
Air Force Data Services Center
Air Force Data Systems Design Center
FEDSIM[1] Center
Air Force Computer Acquisition Office
Major Field Commands
ADP Single Mgr
DPI
1/ FEDSIM - Federal Computer Performance Evaluation and Simulation Center
Command Line
Principal Communications Channel

FIGURE 5

DEFENSE SUPPLY AGENCY ADP PROGRAM



DIDSO-Defense Integrated Data Systems Office
SIMO -SAMMS Program Management Office
DARO -DoD ADPE Reutilization Office
DSAO -Data Systems Automation Office
DAASO-Defense Automatic Addressing Systems Office
DAAF-W - Defense Automatic Addressing Facility-West

FIGURE 6.—CENTRAL SYSTEMS DESIGN AND DEVELOPMENT ACTIVITIES

ARMY

CSC: Computer Systems Command.
ALMSA: Automated Logistics Management Systems Activity.
LSSA: Logistics Systems Support Agency.

NAVY

NAVCOSSACT: Navy Command Systems Support Activity.
OASDO: Computer Applications Support and Development Office.
FMSO: Fleet Material Support Office.
MSDO: Management Systems Development Office.
OENO: Central Naval Ordnance Management Information System (NOMIS) Office.

AIR FORCE

DSDC: Data Systems Design Center.
ALSO: Air Force Logistics Systems Command.
MPC: Military Personnel Center.
AFAFC: Air Force Accounting and Finance Center.

DSA

DSAO: Data Systems Automation Office.

FIGURE 7.—CENTRAL ADPE SELECTION ACTIVITIES

ARMY

CSSEA: Computer Systems Support and Evaluation Agency.

NAVY

ADPESO: Automated Data Processing Equipment Selection Office.

AIR FORCE

ESD(AFSC): Electronic Systems Division (Air Force Systems Command).

DSA

HQ: Headquarters.

FIGURE 8.—SYNOPSIS OF DEPARTMENT OF DEFENSE ADP POLICY ISSUANCES

DoD Directive 5100.40: Responsibilities for Administration of the Automatic Data Processing Program, August 19, 1975, outlines the policy responsibilities for administering the DoD ADP Program. In particular, it designates the Assistant Secretary of Defense (Comptroller) as the Senior ADP Policy Official.

DoD Directive 4105.55: Selection and Acquisition of Automatic Data Processing Resources, May 19, 1972, establishes policies for selecting and acquiring ADP resources in DoD. Among other things, the policy requires that selections of ADP resources are based on well-documented cost effectiveness studies.

DoD Instruction 5010.27: Management of Automated Data System Development, November 9, 1971, establishes policy, procedures and management controls and assigns responsibilities for the development of automated data systems.

DoD Directive 4160.19: Department of Defense Automatic Data Processing Equipment Reutilization Program, April 5, 1973, prescribes Department of Defense policies and assigns responsibilities and authorities governing the DoD Automatic Data Processing Equipment Program and establishes the Defense ADPE Reutilization Manual (DoD 4160.19M) as a regulation of the DoD and assigns responsibility for its development and maintenance.

DoD Instruction 4140.38: Automatic Data Processing Management Information System (ADP/MIS), June 18, 1973, establishes an automatic data processing (ADP) management information system to assure DoD-wide compliance with and reporting of ADP resource information to the General Services Administration (GSA).

DoD Instruction 5030.40: Government-wide ADP Sharing Program, March 27, 1969, establishes policies and procedures governing the utilization of automatic data processing (ADP) resources by means of participation in the Government-wide ADP Sharing Program operated by the General Services Administration (GSA).

DoD Instruction 7900.1: Federal COBOL Compiler Testing Service (FCCTS), May 19, 1976, establishes policy, procedures and management controls and assigns responsibilities for the selection, acquisition, development and maintenance of COBOL Compilers.

DoD Directive 5000.11: Data Elements & Data Codes Standardization Program, December 7, 1964, states the policies and responsibilities governing the Program. The principal policy is that data elements and codes will be standardized in all data systems in order to assure their compatibility.

DoD Instruction 5000.12: Data Elements & Data Codes Standardization Procedures, April 27, 1965, contains the policy that data elements will be standardized using the Assigned Responsible Agency concept. Also prescribes procedures for identification, development, coordination, approval and publication of standards in DoD 5000.12(M).

DoD Instruction 5000.18: Implementation of Standard Data Elements and Related Features, March 27, 1969, contains policies and procedures governing implementation of standards in new data systems when the system is implemented, in on-going data systems on an agreed upon date on a system by system basis. Also states policy on translation and conversion cost payment in data interchange situations when only one system and organization uses standards.

DoD Directive 5160.49: Department of Defense Computer Institute (DoDCI), February 12, 1976, establishes the DoDCI, describes its objectives, and prescribes the functions and responsibilities to include resources support. The DoDCI will provide a central education and training capability abreast of current technology and will be operated by the Navy.

DoD Directive 5200.28: Security Requirements for ADP Systems, December 18, 1972, and DoD Manual 5200.28M, January 1973, ADP Security Manual, establish the DoD ADP Security Program setting forth the security requirements, policy objectives, organizational responsibilities, and structures, protective measures, and implementation, education and testing procedures.

DoD Directive and Manual 4120.17: DoD Automated Data Systems Documentation Standards, December 1972, authorizes the publication of the manual setting forth the 10 types of documentation, requires all ADSs to be documented according to the standards, prescribes the procedures for determining the extent of documentation suitable for each situation, and assigns responsibilities.

DoD Directive 4120.3: DoD Standardization Program, June 6, 1973, and Manual 4120.3M, Standardization Policies, Procedures and Instructions, establishes the DoD Standardization Program, describes the program, assigns responsibilities for each area of standards, and prescribes the procedures for executing the program. The Air Force is "assignee activity" for the DoD category, Information Processing Standards for Computers (IPSC). The Army and Navy are "participating agencies" and the Defense Agencies are liaison agencies.

DoD Instruction 4105.65: Acquisition of Automatic Data Processing Computer Program and Related Services, June 29, 1970, establishes the procedures for defining the requirements and preparing purchase requests for the acquisition of computer programs and related services and assigns responsibilities.

FIGURE 9.—ECONOMIC GUIDANCE PAPERS FOR ADP

1. Reducing Computer Based Printing and Paperwork, September 21, 1973.
2. Vulnerability of ADP Systems to the Energy Shortage and Reducing Consumption of Energy by ADP Systems, January 14, 1974.
3. Uniterruptible Power Supply (UPS) for ADP, May 16, 1974.
4. Improving the Economy of Data Entry Services, November 29, 1974.
5. Contemporary Considerations in Economic Analysis for ADP, March 18, 1975.
6. Program Evaluations of ADP Systems, May 29, 1975.
7. Impact of New ADP Technology, July 22, 1975.
8. Management Considerations in Operating Systems Development and Maintenance, December 17, 1975.

FIGURE 10.—SYNOPSIS OF DEPARTMENT OF ARMY ADP POLICY ISSUANCES

AR 18-1, Management Information Systems Policies, Objectives, Procedures and Responsibilities, March 22, 1976, describes objectives, prescribes policies, assigns responsibilities, and specifies procedures for selection, acquisition, and management of ADPE within the Army.

AR 18-3, Automatic Data Processing Management Information System, November 1971, provides instructions and formats for inventorying ADP equipment and characteristics.

AR 235-5, Management of Resources: Commercial and Industrial-Type Functions, November 1972, which establishes policies, procedures, and responsibilities for determining whether or not commercial and industrial products/services should be procured from: commercial/industrial sources, Army in-house activities, or other Federal Agencies.

AR 37-13, Economic Analysis and Program Evaluation of Resource Management, April 1973, which provides policies and procedures for consistent application of economic analyses within the Army.

AR 18-12, Catalog of Standard Data Elements and Codes, March 29, 1974, describes standard data elements and codes for use in ADP systems.

Economic Analysis of Proposals Supported by Automated Data Systems, Office of the Army Chief of Staff, January 25, 1972, provides a supplement to AR 37-13 and AR 18-1 with respect to economic analyses for ADPE.

FY 1976 ADP Budget, RCS CSCAB—205 (Draft), Office of Army Chief of Staff, March 9, 1976, provides instructions for preparing and submitting the FY 1976 ADP Budget.

AR 18-7, Data Processing Installation Management, Procedures and Standards, June 1976, describes the controls required for the management of operational data processing installations and the procedures and standards that these DPIs are to follow.

FIGURE 11.—SYNOPSIS OF DEPARTMENT OF NAVY ADP POLICY ISSUANCES

SECNAV 5200.18: Data Elements and Data Codes Standardization Program, December 3, 1968, establishes the basic program and implements DoDD 5000.11.

SECNAV 5200.19: Data Elements and Data Codes Standardization Procedures, December 9, 1968, sets forth procedures for creating standard data elements and codes in implementation of DoDI 5000.12.

SECNAV 5200.20A: Catalog of Standard Data Elements and Related Features, March 20, 1972, lists the approved standard data elements and implements DoD 5000.12M.

SECNAV 5200.24: Implementation of Standard Data Elements and Related Features, November 3, 1969, states policy for implementation of standard data elements and implements DoDI 5000.18.

SECNAV 5200.26: Department of the Navy ADP Program; Department-level Procedures, September 25, 1970, describes organizational relationships at the headquarters level for management of the ADP program.

SECNAV 5200.28: Information Processing Standards for Computers (IPSC) Program, September 29, 1971, governs participation in the IPSC category of the Defense Standardization Program.

SECNAV 5230.2: Department of the Navy ADP Management Steering Committee, May 12, 1975, establishes a steering committee for ADP management in the Department of the Navy chaired by the Assistant Secretary of the Navy (Financial Management).

SECNAV 5230.3: ADP Users Group Program, July 25, 1975, provides for Department of the Navy participation in the Defense users groups for IBM 360/370 and Burroughs computers.

SECNAV 5230.4: Department of the Navy ADP Program, May 3, 1976, governs the basic structure of the ADP Program and implements DoDD 5100.40.

SECNAV 5230.5: Department of Defense Computer Institute, May 3, 1976, delegates responsibility for operation of DoDCI to the Chief of Naval Operations, in implementation of DoDD 5100.40.

SECNAV 5231.1: Management of Automated Data Systems Development, February 25, 1972, establishes procedures for management of ADS development and implements DoDI 5010.27.

SECNAV 5233.1A: Department of the Navy Automated Data System Documentation Standards, June 20, 1973, implements DoDI 4120.17 and provides additional guidance on document layout and flow charting.

SECNAV 5234.1: COBOL Compiler Validation, March 2, 1973, implements DoDI 4120.16 and assigns responsibilities within the Department of Navy.

SECNAV 5236.1A: Specification, Selection and Acquisition of ADPE, April 30, 1974, governs procurement of ADPE and implements DoDI 4105.55.

SECNAV 5236.2: ADP Services Procured by Contract, February 13, 1974, governs procurement of ADP software and services, implementing DoDI 4105.65.

SECNAV 5237.1: ADPE Reutilization Program, July 7, 1975, governs reutilization of ADPE and implements DoDD 4160.19.

SECNAV 5238.1A: Department of the Navy ADP Program Reporting System (ADPPRS)—Resources Accounting, February 15, 1973, collects the data for the Government-wide ADP Management Information System, implementing DoDI 4140.38.

SECNAV 10462.16A: Government-wide ADP Sharing Program, December 5, 1969, requires sharing of unused Government capacity prior to acquiring additional capacity, implementing DoDI 5030.40.

SECNAV 10462.18: Department of the Navy ADP Review and Evaluation Program, April 6, 1971, establishes criteria and procedures for assessment of computer installations before and after equipment is brought on board.

OPNAV 5231.1: Automated Data System Development; Procedures for the Management of, May 30, 1972, implements and expands upon SECNAV 5231.1.

OPNAV 5236.1: Specification, Selection, and Acquisition of ADPE, February 25, 1972, implements SECNAV 5236.1A and delegates approval authorities.

OPNAV 5236.2: ADP Services Procured by Contract, July 1974, implements SECNAV 5236.2 and delegates approval authorities.

OPNAV 5510.131: Security Requirements for ADP Systems, June 1, 1973, implements DoDD 5200.28 and establishes Navy ADP security procedures.

OPNAV 10462.8: Standard Higher Level Digital Computer Programming Languages; Policy Concerning, March 13, 1969, calls for maximum programming in standard higher level languages.

Naval Material Command Instruction, NAVMAT 4860.12: Commercial or Industrial Activities Program, January 25, 1972, implements OMB Circular A-76 and DoDI 4100.15 and assigns responsibilities for the commercial/industrial activities program within the Navy.

FIGURE 11.—SYNOPSIS OF MARINE CORPS ADP POLICY ISSUANCES

MCO 4860.3A, Operation of Commercial or Industrial Activities, February 16, 1972, describes guidelines for determining whether in-house or contract services will be used.

MCO P5200.15A, Automated Data Systems Manual (ADSM), June 15, 1973, contains descriptions of ADS.

MCO 5230.2B, Central Design and Programming Activities, November 17, 1975, establishes and provides functions for ADP central design activities.

MCO 5230.5, Management of Automatic Data Processing Equipment (ADPE) at Marine Corps Air Stations, August 19, 1970, describes ADP management procedures.

MCO 5230.7, Marine Corps Automatic Data Processing Management Standards Program, May 29, 1974, promulgates ADP standards for the Marine Corps.

MCO 5230.8, Maintenance and Modification of Automated Data Processing Applications Software, Request for, November 17, 1975, issues policy relative to software maintenance and modification.

MCO 5230.9, Standard Procedures for the Control of Centrally Managed Automated Data Systems, November 17, 1975, describes the procedures for central control of ADS.

MCO 10462.7A, Third Party Computer Maintenance (3PCM), January 16, 1976, promulgates maintenance procedures for 3PCM.

MCO 10462.4A, Use of Automatic Data Processing Equipment (ADPE) for Financial & Related Operations, September 28, 1971, describes financial operations with ADPE.

MC Bulletin 5200, Marine Corps Automated Data Systems Plan (ADSP), FY 75–80, January 15, 1975, describes the MC five year ADP plan.

FIGURE 12.—SYNOPSIS OF DEPARTMENT OF AIR FORCE ADP POLICY ISSUANCES

AFR 23–40, Air Force Data Automation Agency, June 10, 1974, prescribes the mission, organization, operating concepts, and responsibilities of the AFDAA.

AFR 23–41, Air Force Data Services Center, December 19, 1975, prescribes the mission, organization, and responsibilities of the AFDSC.

AFR 23–42, Air Force Data Systems Design Center, November 1, 1972, prescribes the mission, organization, and responsibilities of the AFDSDC.

AFR 23–43, Federal Computer Performance Evaluation and Simulation Center, October 24, 1975, prescribes mission, organization and responsibilities of FEDSIM, including its relationship with other Government and Air Force agencies.

AFM 300–6, Automatic Data Processing (ADP) Resource Management, September 1, 1975, contains guidance and establishes requirements, procedures, etc., for the operation and management of ADP resources.

AFR 300–1, Automatic Data Processing Program Management, November 15, 1974, prescribes policies and responsibilities for the management of the Air Force ADP Program. (Currently under revision).

AFR 300–2, Management of Automatic Data Processing Systems, February 14, 1975, prescribes policies and responsibilities for managing automatic data processing systems. (Currently under revision).

AFR 300–3, Automatic Data Processing Planning, Programming, and Budgeting Information System, March 20, 1974, shows the interface of the Air Force ADP Planning System with the DoD Planning, Programming, and Budgeting System.

AFM 300–4, Data Elements and Codes, dates vary by volume, consists of 12 volumes, which are maintained and published by AFDSDC. AF/ACDX retains policy control only. Vol I is the volume on General Instructions; the other volumes contain data elements and codes for various functional areas.

AFR 300–5, Standardization of Data Elements and Related Features, March 20, 1975, states the objectives, policies, and procedures governing the standardization of data elements and related features.

AFR 300–7, Automatic Data Processing Planning Concepts, April 19, 1974, provides guidance for conducting the planning phase of managing ADP resources. (Currently under revision).

AFR 300–8, Security Requirements for Automatic Data Processing Systems (ADPS), June 3, 1974, provides policy and assigns responsibilities for implementation of ADP security procedures.

AFR 300–10, Computer Programming Languages, October 20, 1971, prescribes policy for computer programing languages.

AFR 300–11, COBOL Compiler Validation, April 12, 1973, prescribes policy relative to COBOL compiler validation within the Air Force.

AFM 300–12, Procedures for Managing Automatic Data Processing Systems, December 10, 1971, prescribes procedures for managing automatic data processing systems. (Currently under revision)

AFR 12–35, Air Force Privacy Program, September 26, 1975, implements the Privacy Act of 1974, and DoDD 5400.11.

AFR 300–13, Safeguarding Personal Data in ADPS, May 14, 1976, provides guidelines for safeguarding personal information in ADP environments.

AFR 26–12, Use of Contract Services and Operation of Commercial/Industrial Activities, January 29, 1974, provides the philosophy, policy, and procedures pertaining to the Air Force utilization of contract services, in consonance with DoD Directive 4100.15 and DoD Instruction 4100.33.

AFM 171–404, ADP Management Information System, Vol II, (continually updated), provides instructions for update of the Air Force ADP management information system.

SYNOPSIS OF DEFENSE SUPPLY AGENCY DATA PROCESSING ISSUANCES

I 4705.1: ASSIGNMENT AND CONTROL OF INTERNAL DOCUMENT IDENTIFIER CODES AND VALIDATION/REASON CODES, 3 SEPTEMBER 69

Purpose: To establish policies and procedures, and assign responsibilities for the assignment and control of Internal Document Identifier Codes (DICs) and Validation/Reason Codes (V/RCs) within DSA.

Scope: This DSA–HSI is applicable to HQ DSA and the Data Systems Automation Office (DSAO).

R. 4705.2: DATA ELEMENTS AND DATA CODES STANDARDIZATION PROCEDURES, 14 SEPTEMBER 65

Purpose: To implement within he Defense Supply Agency (DSA) the Data Elements and Data Codes Standardization Procedures as prescribed by DoD Instruction 5000.11 and DoD Instruction 5000.12 (Encl 1).

Scope: (A) This DSAR is applicable to HQ DSA and all DSA field activities concerned with the development, use and maintenance of data systems for both internal and eternal application in common or specialized functional or mission areas. (B) Data elements to be considered in this effort are those that input or output a data processing system. Data elements which are used as an integral part of a computer program, for example, constants, record storage locations, factors used in computation, and program operation codes are not bound by the criteria of Enclosure 1. Data Elements and Data Codes which are required to be unique for use in technical files of cryptologic activities are excluded.

R 4705.5: IMPLEMENTATION OF STANDARD DATA ELEMENTS, 28 MAY 75

Purpose and Scope: To establish policy and procedures for implementing DoD Instruction 5000.18, Implementation of Standard Data Elements and related Features, into DSA data systems. This DSAR is applicable to HQ DSA and all DSA field activities concerned with the development and maintenance of data systems (both Uniform Automated Data Processing Systems (UADPS) and non-UADPS). Data elements and data codes which are required to be unique for use in technical files of cryptologic activities are excluded from the provisions of this DSAR. However, unclassified output of cryptologic activities are subject to provisions of this DSAR.

R 4710.1: ADMINISTRATION OF AUTOMATIC DATA PROCESSING EQUIPMENT, 21 AUGUST 72

Purpose and Scope: To establish policy, guidance, and procedures for the selection and acquisition of automatic data processing (ADP) resources; assign responsibilities for administering the DSA ADP Program; exploit computer technology; attain optimum uniformity, compatibility, responsiveness, and standardization of Automatic Data Processing Systems (ADPS); eliminate duplication and overlap in ADPE development; establish long range and intermediate objectives; and implement DoD Directives 4105.55 and 5100.40. This DSAR is applicable to HQ DSA, Data Systems Automation Office (DSAO), Defense Automatic Addressing System Office (DAASO), Defense Industrial Security Clearance Office (DISCO), and DSA primary level field activities.

R 3135.2: SITUATION REPORTS (RCS DSA(AR) 377(L–MIN)), 3 JUNE 74

Purpose and Scope: To establish policy, assign responsibilities, and prescribe procedures for the preparation, submission, and dissemination of Situation Reports (SITREPs). This DSAR is applicable to HQ DSA and DSA primary level field activities (PLFAs).

R 4710.2: REVIEW OF DATA SYSTEMS AND AUTOMATIC DATA PROCESSING OPERATIONS, 11 APRIL 67

Purpose: To establish policy and assign responsibilities for review of the effectiveness with which automatic data procsesing (ADP) system objectives are being achieved and the efficiency with which computer operations are being performed at DSA field activities.

Scope: This DSAR is applicable to HQ DSA and all DSA field activities having automatic data processing equipment.

R 4710.4: GOVERNMENT-WIDE ADP SHARING EXCHANGE PROGRAM (RCS DD–DSA(Q)740(GSA)), 2 NOVEMBER 72

Purpose: To establish policy and procedures governing the utilization of automatic data processing (ADP) resources by means of participation in the Government-Wide ADP Sharing Exchange Program (hereinafter referred to as the program) operated by the General Services Administration (GSA).

Scope: This DSAR is applicable to HQ DSA, DSA primary level field activities and defense contractors as defined herein.

R 4710.5: ACQUISITION OF AUTOMATED DATA PROCESSING COMPUTER PROGRAMS AND RELATED SERVICES, 16 SEPTEMBER 70

Purpose and scope: (A) To establish responsibilities and procedures for acquisition of automatic data processing computer programs and related services. DSAR 4710.1 establishes DSA policy to perform ADP computer programming and related services in-house. This DSAR provides the procedural guidance for securing waivers from this policy and for assuring that purchased computer programs and related services are reliable, of uniform quality, and are secured at controlled costs. This DSAR implements DoD Instruction 4105.65 and is applicable to HQ DSA and DSA primary level field activities. (B) The provisions of this DSAR apply to the selection and acquisition of the following computer programs and related services:

1. Any collection of computer programs, related studies or methods, or techniques.
2. Products which have as a major portion the design and development of such computer programs.
3. The documentation supporting, describing, or extending the use of such computer programs.

C. Acquisition of the following computer programs is excluded from the provisions of this DSAR:

1. A computer program delivered with a contract but which is incidental to contract performance.
2. A computer program delivered as part of a study or research activity which is to be used no longer than three months after delivery and which has no readily identifiable substantial use elsewhere in the Government.
3. Computer programs procured as part of commercially available Automatic Data Processing Equipment which are not priced separately from the hardware or covered by a separate contract, and where it is not feasible to select, acquire and manage the computer program development separately.
4. Computer program services acquired by a labor-hours type of contract.

R 4710.7: DSA POLICY CONCERNING COMPUTER PROGRAMMING LANGUAGES, 16 FEBRUARY 1973

Purpose and Scope: To establish policy, objectives, guidance, and procedures, assign responsibilities, and implement DoD 4120.16 regarding computer programming languages used in DSA. This DSAR is designed to improve compatibility and interchangeability of computer programs within and among Automatic

Data Processing Systems (ADPS), reduce reprogramming costs, reduce conversion efforts during transition from one computer to another, minimize retraining of computer programmers, improve program documentation and ensure that all revisions provided by vendors to Common Business Oriented Language (COBOL) compilers remain in compliance with the DoD Standard COBOL. The American National Standard COBOL X3.23–1968 has been adopted as the DoD Standard VOBOL. This DSAR is applicable to HQ DSA, Data Systems Automation Office (DSAO), Defense Automatic Addressing System Office (DAASO), Defense Industrial Security Clearance Office (DISCO), and to all DSA field activities undertaking a task or mission which involves the direct or ultimate preparation of computer instructions (programs) for digital data processing equipment used in processing information, and DSA activities acquiring COBOL compilers through a separate contract; the procurement of a computer system, whether or not separately costed; or an "in-house" development effort.

I 4715.1: REQUESTS BY HQ DSA PRINCIPAL STAFF ELEMENTS FOR AUTOMATIC DATA PROCESSING SERVICES, 31 OCTOBER 1966

Purpose: To provide guidance and procedures for submission, evaluation, and control of requests by HQ DSA principal staff elements for automatic data processing (ADP) services.

Scope: This DSA–HSI is applicable to all HQ DSA principal staff elements.

M 4715.1: SAMMS PROCUREMENT SUBSYSTEM OPERATING PROCEDURES, 1 JULY 1969

Purpose: Provide uniform operating procedures for processing inputs/outputs within the Procurement Subsystem of the Standard Automated Materiel Management System (SAMMS) and prescribe the detailed criteria and operating procedures/options associated with the Procurement Subsystem.

Scope: The scope of this manual contains coding instructions, forms and formats of subsystems, input/output, and other miscellaneous instructions.

R 4720.1: POLICY FOR CONTROL OF COMPUTER PROGRAMS, 30 SEPTEMBER 1964

Purpose: To establish a procedure pending the implementation of the Uniform Automated Data Processing Systems (UADPS) for the control of all actions which require changes in existing computer programs or the establishment of new computer programs at Defense Supply Centers (DSCs) and Defense Depots.

Scope: This DSAR is applicable to HQ DSA, all DSCs, and all Defense Depots.

R 4720.2: CONTROL OF REQUESTS FOR SPECIAL FILE DATA FROM THE DEFENSE LOGISTICS SERVICES CENTER, 20 JULY 1972

Purpose and Scope: To establish policy and assign responsibilities for the control of all actions which require the Defense Logistics Services Center (DLSC) to produce special file data or special statistics. This DSAR is applicable to HQ DSA, HQ DSA field extension offices, and all DSA filed activities.

R 4730.1: DEVELOPMENT AND MAINTENANCE OF UNIFORM AUTOMATIC DATA PROCESSING SYSTEMS, 18 OCTOBER 1967

Purpose: To establish policies, assign responsibilities, and prescribe procedures for the development and maintenance of Uniform Automatic Data Processing Systems (UADPS).

Scope: This DSAR is applicable to HQ DSA and DSA primary level field activities who will install UADPS programs. It is not applicable to one-of-a-kind systems installed at Defense Documentation Center (DDC), Defense Industrial Plant Equipment Center (DIPEC), Defense Logistics Services Center (DLSC) and Defense Supply Agency Administrative Support Center (DSASC).

R 4730.2: AUTOMATIC DATA PROCESSING SYSTEM DOCUMENTATION, 30 APRIL 1969

Purpose: To establish policies, assign responsibilities, and specify standards for the documentation of Automatic Data Processing Systems (ADPS).

Scope: This DSAR is applicable to HQ DSA and all DSA field activities engaged in the development, maintenance, and/or operation of ADPS.

R. 4730.3: MULTIACTIVITY AUTOMATED DATA SYSTEM (MAADS) CHANGE PROCEDURE, 5 MAY 76

Purpose and Scope: (A) To prescribe policy, responsibilities, and procedures for the documentation, submission, review, development, and implementation of routine multiactivity automated data system (MAADS) change requests. (B) This DSAR is applicable to HQ DSA, DSA primary level field activities (PLFAs) utilizing MAADS, and the central design activity (CDA).

R 4730.4: EMERGENCY ALTERATIONS TO UADPS PROGRAMS, 20 MARCH 73

Purpose and Scope: To establish policy and procedures for the identification, reporting, and resolution of system deficiencies causing a Uniform Automatic Data Processing System (UADPS) to be inoperative. This DSAR is applicable to HQ DSA and all DSA field activities operating a UADPS.

R 4730.5: DEFENSE CONTRACT ADMINISTRATION SERVICES TIMESHARING USAGE AND CONTROL, 16 JUNE 75

Purpose and Scope: To establish policy, assign responsibilities and prescribe procedures for the controlled use of Defense Contract Administration Services Region (DCASR) timesharing computer terminals. This DSAR is applicable to HQ DSA and all DCASRs.

I 4730.1: MANAGEMENT OF AUTOMATED DATA SYSTEMS DEVELOPMENT, 30 OCTOBER 70

Purpose and Scope: To assign responsibilities for the implementation of DoD Instruction 5010.27 (Enclosure 1). This DSA-HSI is applicable to all HQ DSA automated data systems.

FIGURE 14.—FUNCTIONAL POLICY GUIDANCE THAT IMPACTS THE ADP AREA

DoD Instruction 7041.3, "Economic Analysis and Program Evaluation for Resource Management," October 18, 1972.
DoD Instruction 4100.33, "Commercial or Industrial Activities—Operation of," July 16, 1971.
DoD Instruction 5010.12, "Management of Technical Data," December 5, 1968.
DoD Directive 5200.1, "DoD Information Security Program," June 1, 1972.
DoD Directive 5630.1, "Programming of Major Telecommunications Requirements," April 24, 1968.
DoD Instruction 5100.66, "Establishment of Policy for, and Administration of, Independent Research and Development Programs (IR&D)," January 7, 1975.
DoD Directive 7000.1, "Resource Management Systems of the Department of Defense," August 22, 1966.
DoD Directive 5400.11, "Personal Privacy and Rights of Individuals Regarding their Personal Records," August 4, 1975.
DoD Directive 5010.19, "Configuration Management," July 17, 1968.
DoD Instruction 5025.9, "Control and Protection of 'For Official Use Only' Information," February 1, 1968.
DoD Directive 5000.29, "Management of Computer Resources in Major Defense Systems," April 26, 1976.
DoD Instruction 5200.21, "Certification for Access to Scientific and Technical Information," December 10, 1968.
DoD Directive 5210.46, "Department of Defense Building Security for the National Capital Region," September 23, 1975.
DoD Instruction 5200.22, "Reporting of Security and Criminal Violations," November 8, 1973.

NOTE.—The above list is not exhaustive but merely gives one a feel for the type of policies that impact the ADP area.

FIGURE 15

PLACEMENT OF AUDIT ORGANIZATIONS IN THE DEPARTMENT OF DEFENSE

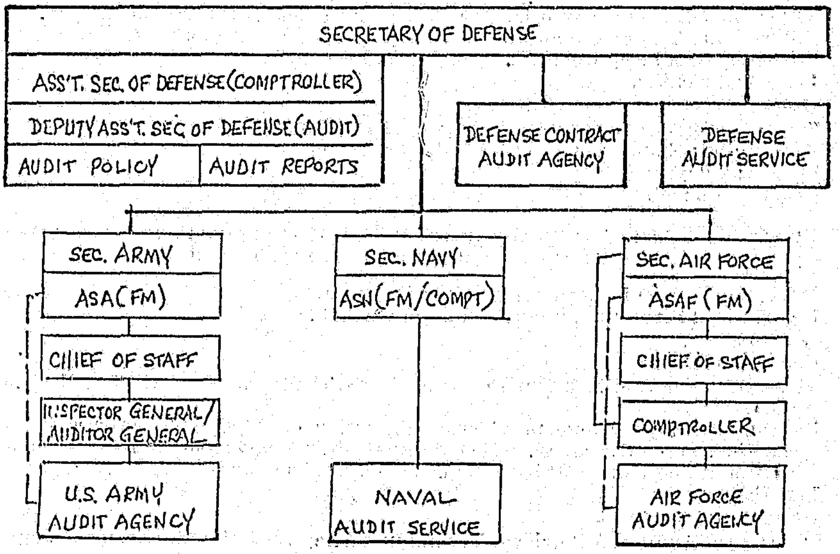


FIGURE 16

ADP TRAINING FOR DOD AUDITORS

	Personnel	
	Number	Percent
Auditors:		
With extensive ADP training and experience	234	10
With some ADP training and experience	1,602	71
ADP specialists	22	1
Total with ADP training and experience	1,858	82
Auditors: With no ADP training and experience	406	18
Total professional personnel	2,264	100
Administrative and clerical	415	
Total combined personnel strength	2,679	

FIGURE 17.—ADP TECHNICAL AND AUDIT TRAINING COURSES CONDUCTED BY OTHER ORGANIZATIONS DURING FISCAL YEARS 1975 AND 1976

ARMY AUDIT AGENCY PARTICIPATION

Title: Computing Systems Fundamentals (Science Research Associates, Incorporated).
Description: A programed instruction course, "Computing Systems Fundamentals" to provide a basic knowledge of computing systems, terminology, programing and numbering systems.
Length: 3 days.
Grade Levels: 5 to 11.

Title: Computer Systems (George Mason University/Monmouth College).
Description: A study of the function, parts and capabilities of a computer system in management.
Length: 3 months.
Grade Levels: 9 to 11.

Title: Introduction to Information Processing (East Carolina University).
Description: To provide an overview or perspective to computer data processing technique and requirements.
Length: 3 months.
Grade Level: 9.

Title: Conference on Computer Software Management (AIAA).
Description: Empasis on the DoD Software Management Plan.
Length: 2 days.
Grade Level: 14.

FIGURE 17A.—ADP TECHNICAL AND AUDIT TRAINING COURSES CONDUCTED BY OTHER ORGANIZATIONS DURING FISCAL YEARS 1975 AND 1976

Title: Seminar on Programming (Yourdin, Inc.).
Description: Structured programming in COBOL.
Length: 2 days.
Grade Level: 13.

Title: ADP for Auditors Course (Army Logistics Management Center, Fort Lee, Va.).
Description: This course provides a discussion of ADP tech-analyses in flow charting, system security, economic analysis, management and utilization of ADP and audit of ADP base management/controls are presented.
Length: 2 weeks.
Grade Levels: 9 to 13.

Title: ADP Audit and Retrieval Technique (Army Logistics Management Center, Fort Lee, Va.).
Description: This course teaches advanced computer concepts and auditing techniques related to computer-based data processing systems. ADP management and audit controls are discussed in detail; students compare and retrieve data using the Army Uniform Data Inquiry Technique.
Length: 1 week.
Grade Levels: 9 to 13.

Title: ADP for Audit Executives (Army Logistics Management Center, Fort Lee, Va.).
Description: This course presents ADP technology, the various facets which comprise an ADP system, and auditing techniques relative to computer-based data processing systems.
Length: 1 week.
Grade Levels: 14 and above.

FIGURE 17B.—ADP TECHNICAL AND AUDIT TRAINING COURSES CONDUCTED BY OTHER ORGANIZATIONS DURING FISCAL YEARS 1975 AND 1976

Title: Computer Orientation for Senior Executives (DoD Computer Institute).
Description: The course covers computer capabilities, limitations and applications to include key concepts and planning factors for establishing new computer systems or improving existing computer configurations.
Length: 1 to 3 weeks.
Grade Levels: 15 and above.

Title: Computer Systems Privacy Course (Civil Service Commission).
Description: This course develops an understanding of the types of action necessary to design, manage and protect the automated "system of records."
Length: 3 days.
Grade Level: 11.

Title: Management Introduction to ADP (Civil Service Commission).
Description: The seminar is designed to provide a management overview of the fundamentals of ADP. It is also the recommended introductory course for participants planning to attend later ADP seminars.
Length: 3 days.
Grade Level: 11.

Title: Introduction to ADP (Civil Service Commission).
Description: An introduction to ADP provides introductory knowledge about the uses and potential of ADP Systems.
Length: 5 days.
Grade Level: 11.

Figure 17C.—ADP Technical and Audit Training Courses Conducted by Other Organizations During Fiscal Years 1975 and 1976

Title: ADP for Administrative, Clerical and Secretarial Personnel (Civil Service Commission).
Description: Introductory course on basic concepts of ADP and the terminology of the computer profession.
Length: 3 days.
Grade Level: 5.

NAVAL AUDIT SERVICE PARTICIPATION

Title: Basic COBOL (Honeywell).
Description: Course covered programming language of Honeywell 6000.
Length: 5 days.
Grade Levels: 12 to 14.

Title: EDP International Conference (EDP Auditors Association).
Description: Course covered data processing in auditing field.
Length: 2 days.
Grade Levels: 12 to 14.

Title: Introduction to DS/VS for Managers and Analysts (IBM).
Description: The course is an introduction into the new techniques being developed by IBM.
Length: 3 days.
Grade Level: 14.

Figure 17D.—ADP Technical and Audit Training Courses Conducted by Other Organizations During Fiscal Years 1975 and 1976

Title: Auditing Technique for ADP Systems (Civil Service Commission).
Description: This course provides application of tools, techniques and methods of ADP.
Length: 3 days.
Grade Levels: 11 to 13.

Title: Techniques of File Design and Data Base Structure (Civil Service Commission).
Description: Course covers various concepts in data base and files.
Length: 9 days.
Grade Levels: 11 to 13.

Title: GAO Information Systems Program (Wharton School, U. of Pennsylvania).
Description: To educate selected personnel in the skills required to design, implement, and evaluate advanced information systems.
Length: 20 days.
Grade Levels: 13/LCDR.

Title: ADP Aspects of the Privacy Act of 1974 (DoD Computer Institute).
Description: To provide general knowledge of Privacy Act.
Length: 2 days.
Grade Level: No Requirement.

Figure 17E.—ADP Technical and Audit Training Courses Conducted by Other Organizations During Fiscal Years 1975 and 1976

AIR FORCE AUDIT AGENCY PARTICIPATION

Title: Effective Use and Application of Minicomputers (Air Force Data Systems Development Center).
Description: Minicomputers require a different approach for business applications than what is used for other minicomputer applications and/or other larger scale computerized business systems. This seminar concentrates on developing and appreciation for the differences and varieties of minicomputers available

for business applications and on building some practical guidelines for effective selection, design, development, installation and utilization of minicomputers in a business environment. Some time was spent during the seminar discussing the attendees situations and potential approaches that can be taken to minicomputer utilization.

Length: 5 days (34 hours).

Grade Levels: 9 to 12/Lt-Capt.

Title: File Organizations and Access Methods Seminar (Air Force Data Systems Development Center).

Description: The seminar will consist of lectures and discussions covering the following areas: Generations of System Design, Basic File Attributes, Sequential Processing, Key Transformation/Randomizing, Directories-Indexing, Bit Vector/Matrix, Embedded Link Structures, Inverted File/Index Structures, and Conditional Retrieval Techniques.

Length: 2 days (8 hours).

Grade Levels: 7 to 12/TSgt-Capt.

Title: Parmis II Familiarization (Air Force Data Systems Development Center).

Description: Instruction includes a step by step progression of the initiation, selection, and subsequent working of a PARMIS project. Included is a history of the need and subsequent selection of PARMIS as a management information system.

FIGURE 17F.—ADP TECHNICAL AND AUDIT TRAINING COURSES CONDUCTED BY OTHER ORGANIZATIONS DURING FISCAL YEARS 1975 AND 1976

(A description of the forms and internal use of the system is included.)

Length: 3 days (12 hours).

Grade Levels: 7 to 12/TSgt-Capt.

Title: Decision Logic Tables. (Air Force Data Systems Development Center).

Description: The course is designed to take the student from the basic elements of a DLT through the process of building his own DLT. Each basic element will be presented in detail and built from prior knowledge obtained in previous elements. Two techniques for developing DLTs (Classical and Progressive) will be presented. The three types of DLTs; Limited, Extended, and Mixed; will be defined and developed. Rules and methods of evaluating a DLT for correctness will be presented and applied.

Length: 3 days (12 hours).

Grade Levels: 7/TSgt.

Title: Data Processing Concepts (VAI) (Air Force Data Systems Development Center).

Description: Includes instruction in the area of computer hardware and the five basic components of a computer. It also instructs on the conversion of decimal numbers to binary, octal and hexidecimal and back to decimal. There is instruction in the concept of the stored program which will contain a brief introduction to a programming language. Instruction is also provided to familiarize the student with both real-time and batch processing methods.

Length: 12 hours.

Grade Levels: 12/Capt.

FIGURE 17G.—ADP TECHNICAL AND AUDIT TRAINING COURSES CONDUCTED BY OTHER ORGANIZATIONS DURING FISCAL YEARS 1975 AND 1976

Title: Data Base Management Concepts (Air Force Systems Development Center).

Description: The course will consist of lectures and discussions covering the following areas: Introduction to Data Base Management, Data Organization, Data Base Design, and Date Base Administration.

Length: 5 days (20 hours).

Grade Levels: 12 to 13/Capt.-Maj.

Title: Auditing Data Processing Systems (Air Training Command).

Description: Provides professionally qualified Air Force Audit Agency (AFAA) personnel with knowledge and technical skills necessary to perform effective audit analysis and evaluation of operational automated data processing systems. Training includes ADPS concepts and documentation techniques, computer processes, programming techniques, and specific ADPS audit tools and techniques.

Length: 15 to 18 days.
Grade Levels: 5 to 11/E3-6/Lt-Maj.

Title: Supply System Management (Air Training Command).
Description: Course presents principles of supply organization, UNIVAC 1050–II Computer system, record management financial management, maintenance support functions, stock control, equipment management, material facility functions, inventory procedures, and document control. Transaction processing, document flow, and record update will be addressed.
Length: 13 days.
Grade Levels: 5 to 11/E3-7/Lt-Capt.

FIGURE 17H.—ADP TECHNICAL AND AUDIT TRAINING COURSES CONDUCTED BY OTHER ORGANIZATIONS DURING FISCAL YEARS 1975 AND 1976

Title: Advanced Data Processing Audit Analysis (Air Training Command).
Description: Provides professionally qualified Air Force Audit Agency (AFAA) personnel with the highly specialized knowledge and tech skills necessary for appraising and evaluating the development, testing, and implementation of newly designed or substantially modified automated data systems. The scope of training includes review of computer processes, advanced computer programming techniques, ADPS audit theory, tools, and techniques, and in-depth analysis and evaluation of theoretical data systems.
Length: 30 days.
Grade Levels: 5 to 12. Lt-Maj.

Title: Computer Systems Analyst (Air Training Command).
Description: Techniques of computer applications system and design steps of a system study; project management techniques; flowcharting techniques; file organization; forms design; audit and security control; economic analysis; decision logic tables; development of complete system document; and management of system development activities.
Length: 25 days.
Grade Level: 7, Lt-Capt.
Title: Auditing the Computer Environment (Institute of Internal Auditors Seminar).
Description: To present knowledge on audit of EDP operations, EDP system security, EDP audit packages, and training of EDP audit personnel.
Length: 1 day.
Grade Levels: 13 to 14.

FIGURE 17I.—ADP TECHNICAL AND AUDIT TRAINING COURSES CONDUCTED BY OTHER ORGANIZATIONS DURING FISCAL YEARS 1975 AND 1976

AUDITOR GENERAL-DEFENSE SUPPLY AGENCY PARTICIPATION

Title: Computer Programmer (Defense Supply Agency).
Description: Course consists of programmed instruction and practice problems in ADP.
Length: 1 month.
Grade Levels: Various.

Title: DSA Intra-Agency Recurring Course (Defense Supply Agency).
Description: Technical and operational training in ADP.
Length: 4 months.
Grade Levels: 5 to 7.

Title: EDP Audit and Control I and II (Institute of Internal Auditors).
Description: To review audit problems in computer systems.
Length: 1 week.
Grade Level: 14.

DASD (AUDIT) PARTICIPATION

Title: Computer Dynamics in Management (Oklahoma University).
Description: Course covered the dynamic evaluation of the computer and its impact on management.
Length: 1 week.
Grade Levels: 12 and above.

CONTINUED

2 OF 4

FIGURE 17J.—ADP TECHNICAL AND AUDIT TRAINING COURSES CONDUCTED BY OTHER ORGANIZATIONS DURING FISCAL YEARS 1975 AND 1976

Title: Introduction to COBOL (Naval Audit Service).
Description: Introduction to basic COBOL computer programming.
Length: 5 days.
Grade Levels: 9 to 15.

Title: ADP for Auditors (Army Logistics Management Center, Ft. Lee, Va.).
Length: 10 days.
Grade Levels: 11 to 13.

FIGURE 18—TECHNICAL MEMORANDUM

Subject: Brief Description of NRL's 1974 Computer Penetration Exercise.

BACKGROUND

The Operating System (OS) of a large, modern computer is the program that manages the resources of the computer. Because the operating system normally has complete control over all system resources, a flaw in OS security can lead to violations of the security and privacy of data stored on the system by different users.

Modern operating systems comprise many large programs that interact in extremely complicated ways. For example, the operating system for the UNIVAC 1108 computer, called EXEC VIII, has over 500,000 lines of code and was developed by hundreds of programmers. It is impossible for any one individual to understand such large and haphazardly constructed systems; hence, security loopholes are inevitable. The penetration of EXEC VIII, performed by NRL in 1974, was carried out in order to demonstrate the assertion that these loopholes can be found and exploited easily by knowledgeable people who have access to the system. Although the truth of this assertion is generally agreed upon by experts in OS security, and although a number of successful penetrations had been accomplished by authorized as well as unauthorized teams, in 1974 there were no well-documented demonstrations of the vulnerability of such large scale operating systems as EXEC VIII. This lack of well-documented penetrations was an additional motivation for the exercise conducted by NRL. The penetration exercise was part of a larger effort to evaluate the overall security of the target computer system in accordance with existing Navy instructions.

DETAILS OF THE PENETRATION

Among the security functions that an operating system should provide, two stand out:

(A) The prevention of system use by unauthorized users.

(B) The prevention of security or privacy violations by authorized users (e.g., preventing one authorized user from reading or modifying the files of another authorized user without that user's permission).

Because NRL was an authorized user of the target UNIVAC 1108, the penetration tested the second of these two functions.

The UNIVAC 1108 is typical of large scale, third generation, multiple access systems. In a multiple access system, many users have simultaneous access to the system and are given the appearance of their own dedicated computer by means of time-sharing the single system's resources. In such systems users frequently run programs that are provided by the system for "public" use. Examples of system-provided programs include compilers for programs written in such languages as FORTRAN or COBOL, arithmetic function packages, editors that assist users in modifying their files, etc. Because many users will execute the same copy of these system-provided programs, there is a potential danger that their use will lead to security violations. To avoid violations, the system managers must ensure that these system-provided programs are trustworthy before they are placed on the system and made available to users, and they must ensure that these system-provided programs cannot be modified by users once they are made available. If the latter cannot be ensured, it may be possible for one user to modify a system-provided program so that the next user of that program is the victim of a security penetration. This is exactly what occurred in the NRL penetration.

NRL developed a program that would make use of one of these system-provided programs in a manner that forces an error condition to occur. Because of a loophole in the mechanisms that enforce the OS security functions, this error condition allowed the NRL program to modify the system-provided program. The NRL program would then modify the system-provided program so that, in addition to its normal functions (which were left unmodified), the system-provided program included calls to other NRL programs. These other NRL programs were designed to victimize unsuspecting later users of the now-modified system-provided program. When a later user called such a modified system-provided program, the program would perform its usual functions (which had not been affected) and then call the NRL programs. Because the NRL programs were called indirectly by another user (the "victim"), the operating system treated their execution as part of the victim's own computer run. In this way, NRL programs were able to assume temporarily the identity of the victim. With this disguise, the NRL programs could then take any action normally permitted to the victim, such as copying or modifying the victim's files. The action taken by the NRL programs was to copy those files of the victim that were classified and then to return to the system-provided program that had been called by the victim. Because the NRL penetration did not interfere with the normal functions of the system-provided program, the victim's run was then resumed without visible effects other than a slight delay and a slight increase in the amount charged by the billing programs to the victim's account.

The penetration was accomplished with about four man-months of effort by persons highly trained as systems programmers and familiar with UNIVAC operating systems. The penetration technique itself was demonstrated within two to three man-weeks; the additional effort was expended in order to ensure that the stealing of files would be covert. The final programs managed to avoid having any entries written in the system log that would make the method discoverable after the fact.

Because the purpose of the NRL penetration was to demonstrate feasibility, the NRL programs did no more than steal copies of victims' files (approximately two million words were stolen). The programs, however, could have destroyed or selectively modified the victims' files.

Figure 19

TECHNICAL SECURITY DISPARITY

Case	Estimated cost to obtain per system (in thousands)	Estimated cost to penetrate
A. "As is" systems	0	$3,000
B. Repaired systems	$500	8,000
C. Selective reimplementation	1,500–2,500	100–250,000
D. Redesign and reimplementation	10,000	(1)

[1] Blocked (theoretically).

Source: Air Force Computer Security Technology Planning study panel.

The Computer in White Collar Crime

The first two sections of this chapter of the staff study dealt, first, with the computer security precautions used at the Central Intelligence Agency; and, second, with ADP security procedures at the Department of Defense and certain of its components. Later sections of this chapter of the staff study will examine computer security and computer crime from the point of view of the Department of Justice and then the Department's Federal Bureau of Investigation. The final sections have to do with the Department of Health, Education, and Welfare.

Now, however, before moving to the Federal criminal justice system, the staff study will examine two subjects which are included at this point so that the Justice Department's and the FBI's comments may be seen in better perspective. The two subjects to be examined, in this section and in the section that immediately follows it are "The Computer in White Collar Crime" and "Present Laws That May Apply to Computer Abuse."

This section, "The Computer in White Collar Crime," is based on information and opinions provided the Senate Government Operations Committee, at the staff's request, by August Bequai, former chairman of the Federal Bar Association's Subcommittee on White Collar Crime, a former attorney in the Division of Enforcement at the U.S. Securities and Exchange Commission and an adjunct professor of criminal law at American University's Center for the Administration of Justice.

In the information and opinions provided the committee by Bequai, he spoke frequently of white collar crime but did not define it. The staff of the Senate Government Operations Committee has used a definition of white collar crime offered in a publication entitled "The Nature, Impact, and Prosecutions of White-Collar Crime" (May 1970) by Herbert Edelhertz, a former chief of the fraud section of the Criminal Division of the Justice Department. Edelhertz wrote his study in a project sponsored by the National Institute of Law Enforcement and Criminal Justice, the research arm of the Law Enforcement Assistance Administration (LEAA). Edelhertz defined white collar crime as "an illegal act or series of illegal acts committed by nonphysical (that is, nonviolent) means and by concealment or guile, to obtain money or property, to avoid the payment or loss of money or property, or to obtain business or personal advantage."

August Bequai, who is presently a practicing attorney in Washington, D.C., said white collar crime is growing in the United States and that it costs the American public more than $40 billion a year. This figure, he said, did not include the cost of investigating and prosecuting these offenses. Moreover, one of the more serious facets of white collar crime involves the computer, Bequai said.

Unfortunately, Bequai said, the role of the computer in white collar crime has attracted little attention from law enforcement agencies, at both the Federal and local levels. Few, if any, resources have been committed by appropriate authorities to understand and control computerized white collar crime, Bequai said. He said the preliminary staff investigation of the Senate Government Operations Committee into computer crime was one of the few attempts in the public sector to make a comprehensive review of this problem.

Bequai cited two recent instances of white collar computer crime. These examples served to demonstrate how computerized crime occurs and "the inability of the system to combat it," he said. Recently, the district attorney for Nassau County, N.Y., announced the arrest of the former supervisor of accounts receivable for the Government Employees' Insurance Company on charges of embezzling a large amount of money from that firm, Bequai said. The executive had put false vouchers through the company's computer, Bequai said. As a result, Bequai explained, the computer issued a series of checks made out to a "dummy" company that was controlled by the defendant. Bequai said the former insurance executive would then take checks issued to the dummy company and cash them. The scheme was uncovered, Bequai said, when a clerk noticed that several of the checks being sent to the dummy company were about twice as much as the average checks the insurance firm normally paid out. "By accident, the criminal fell into the hands of the law." Bequai said.

In another case, Bequai said the chief teller of the Union Dime Savings Bank in New York City was charged with stealing more than $1.5 million. The teller initiated the thefts, Bequai said, by transferring funds from legitimate accounts in the bank's computer system to fraudulent accounts and then withdrawing the money from the fraudulent accounts in some form of negotiable instrument. In summary, Bequai said, the money was transferred from the bank's computer system in an electronic funds transfer, then converted to real cash in the fraudulent account. Bequai said the teller was able to redeposit the electronic funds back into the computer system at times of quarterly interest payments to make the affected accounts balance correctly.

The U.S. Chamber of Commerce estimates that computer crimes cost the American public more than $100 million a year, Bequai said. He said that experts agree that computer fraud is increasing and that the probability of such a crime being uncovered is 100 to 1 against detection.

Even when a computer crime is uncovered, Bequai said, and a suspect found, prosecution is difficult. Once convicted, the violator is likely to receive a light sentence because there are too many judges who still view computer crimes "through the eyes of an antiquated legal mentality," Bequai said.

Bequai said computer technology is rapidly advancing beyond the ability of the average citizen to understand. He said, for example, that the IBM-370 computer has a storage capacity 7,000 times that of the UNIVAC I, the first commercial computer. "Our society is fast becoming more and more technological," Bequai said, explaining that these technical changes are having significant impact on crime and the ability of government to control it. "The days of the 'cop on the beat' will become fewer and fewer," Bequai said. "Criminals of the future will steal electronically. Today's criminal may indeed soon become archaic. Law enforcement must also keep up with the pace of this new frontier. The prosecutor and the investigator of the near future will need training in this new area of crime. At present, there is no such blueprint. Whatever training now exists, it's limited and also too superficial. If we are to win this battle, much more will be needed."

Bequai said computer crimes can be categorized into one or more of the following areas: (1) financial crime; (2) property crimes; (3) information crimes; (4) theft of services; and (5) vandalism.

Financial crimes involving the computer are executed most successfully by violators who are able to penetrate ADP systems having to do with payrolls, accounts payable and receivable, storage and maintenance of files of financial data, and other forms of financial processing.

Bequai said an insightful illustration of financial crime by computers was the Equity Funding fraud, "The giant west coast conglomerate, where more than 60,000 of a total of 97,000 [insurance] policies were created and recorded in the invisible computer files assigned to

'Department 99.' The '99' designation enabled the computer billing programs to skip the bogus policies when the bills were sent to policyholders."

Bequai said the equity funding scheme was revealed neither by an audit nor by State or Federal investigators but rather by a disgruntled ex-employee. Ultimately, Bequai said, the scandal cost policyholders and others more than $2 billion, constituting the biggest fraud "in the annals of crime . . . made possible by the aid of computers." The equity funding scheme, exposed in 1973, and other frauds of smaller but related modes have demonstrated the existence of computerized financial crime but, as yet, law enforcement officers are not being adequately trained to detect or prosecute them, Bequai said.

Bequai then commented on the next category of computer crime, those having to do with property. In these instances, Bequai said, the violator usually takes merchandise or other property for resale. He said that several years ago a student at the University of California found a set of computer system transactions in a trash bin. The system transactions belonged to the Pacific Telephone & Telegraph Co.

Using a touch-tone telephone and the code he had found in the trash bin, the student began placing orders with the company's computer for various products, Bequai said. The student had learned from the system instructions that Pacific Telephone allowed for a certain amount of quarterly loss for each location. Bequai said that, in addition, the student was able to learn from the company computer what products were being ordered from each of the firm's supply locations. The student was thus able to keep his orders, or thefts, within the loss allowance of the phone company, Bequai said, adding that the student had stolen more than $1 million in property before he was discovered. "Once again," Bequai said, "not law enforcement, but rather a disgruntled associate blew the whistle."

Next, Bequai discussed computer crimes involving information. These crimes, he said, take the form of unauthorized access to the computer system—and the data contained therein—by use of a remote terminal. Bequai said this method of gaining unauthorized access to computerized data can be perpetrated when the computer services and physical facilities are available to employees during nonworking hours or when the computer programs and files are insufficiently protected.

In one such instance, Bequai said, three computer operators at offices of a major educational publisher copied nearly 3 million names from a computer file that contained the names of the firm's "most valued" customer list. The violators then sold the customer list to competitors of the firm, Bequai said. In a second case of a computer information access crime, Bequai described a scheme in which violators stole the 5-year marketing plans of a major international airline company and sold the plans to a competitor of the firm. "In both cases," Bequai said, "no one was ever prosecuted. In the latter case, the company has never admitted the theft. Firms are reluctant to tell the public they've been 'had.' "

There could have been safeguards built into the computer systems of both of the victimized companies that might have prevented the crimes, Bequai said. Fingerprinting and background checks of computer system personnel might have revealed that certain employees had criminal records, he said. He also proposed a form of licensing of personnel with access to a computer system that might "filter out undesirable elements." "However," Bequai said, "law enforcement must possess the capability to investigate and prosecute such crimes. It must win the confidence of both industry and public, if individuals are to come forth and testify."

The fourth form of white-collar crime involving computers cited by Bequai has to do with theft of services. This form of theft often surfaces when the computer time of businesses and other institutions is used by persons for their own profit without the knowledge of the organizations which control the ADP equipment and software. Bequai said that frequent victims of this kind of crime are universities and computer-service centers. Bequai cited one analyst-programmer who was discovered to be using his employer's computer to run his own business. "There have been cases where candidates for political office have used a city's computer for direct mail purposes," Bequai said, adding that security measures could be readily devised and put in place to control this kind of crime if institutions vulnerable to such compromise would take appropriate action.

Vandalism was the final form of crime involving computers discussed by Bequai. Violators in this kind of crime do not use the computer or its services for profit but, instead, Bequai said, the computer itself becomes the target of a destructive act. Data contained in the computer system, particularly an organization's recordkeeping procedures, may be intentionally damaged, Bequai said. Vandals may include an angry employee, adversaries in a labor-management dispute, or politically motivated persons who may be extremists "or even saboteurs from an enemy nation," Bequai said. Demonstrating the significant damage one disgruntled worker may cause, Bequai cited a case in which one employee removed the labels on 1,500 reels of computer tape. The act cost the company thousands of dollars in costs and man-hours in reidentifying the data, Bequai said.

Having described the five principal methods, and combinations thereof, of computer white-collar crime, Bequai then sought to explain why computers lend themselves to criminal attack. He said more than 80 percent of American businesses depend in one form or another on computer technology. He said persons knowledgeable in the size and scope of computer operations in the United States have estimated that the crippling of 100 key computers in this country could damage the activities of businesses in States throughout the Nation. Bequai noted—as has been asserted earlier in this staff study by other experts—that, just as American business depends on computers, Government similarly relies on computers.

Bequai said that computers have also grown in storage capacity. Today's generation of computers can store more than 5,000 times as much data as those of 20 years ago. "They can add and subtract, and perform many other feats at speeds many times greater than their predecessors," Bequai said.

But, he said, despite the advances in computer technology, the computer remains fundamentally a system with five key areas of operation—and law enforcement officers and others in the criminal justice system must recognize that it is in these five crucial areas of operations where criminal penetration attempts are likely to occur.

In turn, he said, law enforcement personnel should be trained in the rudiments of these five operating areas.

The first stage, he said, is the "input phase." At this level, data is translated into a language that the computer can understand. Many computer crimes depend on the manipulation of input data. Bequai said criminals can introduce false records, or alter current data by removing key input documents, or do a combination of both. In a case described by Bequai, a vice president of a major manufacturing firm inserted fraudulent data into the computer, thereby creating fictitious suppliers and truckers. About $1 million in corporate checks were then issued by the computer to these fictitious firms, Bequai said. Ironically, the vice president had, on several occasions prior to the discovery of his fraud, been honored for distinguished service to the firm. Bequai said this fraud demonstrates the lesson in law enforcement that agents making inquiry into reported computer crime should always interview all individuals who have had access to the computer input phase and also review any and all logs, records and other "audit trails" indicating a record or pattern of computer access. Internal audit efforts should also be initiated on a "spot check" basis to detect any "dummy" accounts.

From a crime prevention point of view, the second key phase of computer operations which should be understood by investigators is the "programing" stage. During this stage, Bequai said, the computer is provided with step-by-step instructions for solving problems it may encounter. At this phase, Bequai said, the computer criminal can program the ADP system to operate in the fashion he instructs it to. The violator may also alter or delete the program, or even destroy it, Bequai said. He cited an instance in which an accountant for a firm altered a computer program so that a few pennies were added to the cost of many purchased items. The accountant converted the excess pennies into a profit of about $1 million over a period of 5 years. He did this, Bequai said, by converting bookkeeping entries, creating fictitious suppliers and issuing checks to them. Under a number of assumed names, the accountant then withdrew the funds from bogus checking accounts he had set up, Bequai said.

The programing stage of the computer's operations is also vulnerable to simple theft, Bequai said, explaining that one employee of a manufacturing firm tried to sell his employer's computer programs to a competitor for several million dollars.

The third stage of computer operations that can be penetrated by violators is the "central processing unit" or CPU, Bequai said. "The CPU is the computer's memory bank or brain," Bequai said. "It responds to problems the computer faces based on instructions it receives from the program." Bequai said the CPU can be a target for either criminal or terrorist attack as well as sabotage.

Concerning the CPU, Bequai went on to say:

> Criminals may also "wiretap" the system. This involves connecting a tap directly to the telephone or teleprinter lines in order to intercept and record messages. Criminals can also intercept the radiation generated by the CPU. The system is also open to attack from "browsing"—typing an unauthorized terminal into it. The browser gains entry into the system and

> then manipulates it for his own ends. The criminal will usually probe for weak or unprotected points. Once he finds these, he will then attack the computer through one or more of the ways already discussed.

Bequai concluded his comments about the central processing unit by saying that experts estimate that a firm with more than 90 percent of its records computerized will not be able to continue doing business if the CPU is destroyed.

A fourth and vital area of computer operation vulnerable to compromise, Bequai said, is the "output phase." In this process, he said, data from the CPU is passed on and translated in an intelligible form for the user to understand. This data is vulnerable to theft or manipulation. Bequai reported one case in which a computer operator in a medium-sized firm prepared a duplicate time card for a shipping department employee. The dishonest computer operator processed the data with the regular payroll data. However, he instructed the computer to omit listing certain details concerning the second or duplicative check. But the second check was included in the overall check payout totals, Bequai said. The checks were signed mechanically and were totaled to prove that the amounts paid out agreed with the total on the payroll register. Bequai said that the computer operator removed the computer-generated duplicate check. Then the computer operator forged the employee's signature and cashed the check. Bequai said the computer operator separated this scheme many times. The computer operator used the names of different employees from different departments from within the firm. "By so doing, he minimized the chances that these employees would notice the increase in their year-end statement of earnings," Bequai said.

Bequai said it should be noted that thefts of computer printers, mailing lists, customer lists and confidential marketing data also occur during the output phase of the computer's operations. "These may find their way into the hands of competitors and also possibly foreign powers, especially where the firm is engaged in defense work," Bequai said.

The fifth and final stage of a computer's operations that is vulnerable to criminal attack involves the "communication of data," Bequai said. This stage of ADP work requires the use of telephone circuits, or teleprinter lines, to transmit data back and forth between computers and between computers and remote terminals, Bequai said. He added that data communication can also occur between a remote terminal located within a company and a time-sharing service bureau it uses; or between a remote terminal and a company owned computer, Bequai said.

The form of attack in the data communication phase was termed "telephonic penetration" by Bequai. In this process, Bequai said, the criminal gains access to a targeted computer and engages in unauthorized processing and copying. The violator may also alter data or create bogus data. Bequai said the violator may use various methods to achieve "telephonic penetration," including wiretapping, electromagnetic pickups, browsing and "trap door entries," Bequai said.

Wiretapping in computer terminology is defined first as "active wiretapping" which is the attaching of an unauthorized device, such as a computer terminal, to a communications circuit for the purpose of obtaining access to data through the generation of false messages or control signals, or by altering the communications of legitimate users; and second as "passive wiretapping" which is the monitoring or recording of data while the data is being transmitted over a communications link.

"Electromagnetic pickups," in computer terminology, have to do with signals transmitted as radiation through the air and through conductors.

"Browsing" was defined earlier in this section of the staff study and "trap door entries" describe a situation in which, owing to instructions fed into a system, a breach is created intentionally in an ADP system for the purpose of collecting, altering or destroying data.

It was Bequai's view, articulated at the beginning of this section, that once a suspected computer criminal is caught, prosecution is complicated and not always dealt with effectively. "Computer frauds are not only difficult to detect, but the prosecution of those engaged in them may also prove equally difficult given our present evidentiary system," he said. For that reason, he said, prosecutors and investigators should, whenever possible, concentrate on developing their cases in areas not involving computer-generated evidence.

Experts differ on how well the existing legal structure can accommodate computer litigation, Bequai said. The majority take the position that, at best, such litigation is hard for judges and juries to understand. Others take the view that the present legal system is sufficiently flexible to deal with computer-related prosecutions, Bequai said.

The hearsay issue raises special questions for trials. Bequai said, "Hearsay evidence is testimony in court or written evidence of a statement made out of court and offered to establish the truth of the matter asserted." Computer records, Bequai said, whether they are printouts or reels of tape, thus fall under the hearsay rule as being evidence of a written statement made out of court. He noted exceptions to the hearsay rule which are directed toward bringing in reliable data and excluding the unreliable. Accordingly, he said, computer-generated evidence would have to be brought into court under one of these exceptions.

Bequai said that under the common law regular business entries were introduced into court under the "shop-book-rule." He said the present Federal Business Records Act has codified this rule for Federal courts. The majority of States have adopted a similar provision, the Uniform Business Records as Evidence Act, Bequai said, adding that this act places substantially the same requirements as the "old shop-book-rule."

Bequai explained:

> All these rules have one objective in mind: allow a business record to be introduced into evidence if it proves to be reliable. To prove itself reliable it must meet certain criteria: (1) it must be made routinely during the course of business; (2) it must be entered contemporaneously or within a reasonable time after a transaction is recorded; (3) it must have

> been entered by a person who must have had personal knowledge of the event being transcribed; (4) it must have been entered by a person who is unavailable as a witness; and (5) that individual must have had no motive to misstate.

In light of those five criteria, Bequai said, the problem with computer-generated evidence is that such evidence may not have been entered contemporaneously but rather many hours or days afterward; and it may have involved a number of persons, many or all of whom may have had no knowledge of the event from their own personal contacts. It should be further noted, Bequai said, that computer records can be easily altered both before and after they are entered into the computer. Courts are fully aware of the ease with which computer records can be changed and, therefore, are "reluctant to ease the evidentiary rules," he said.

Bequai said the leading case dealing with computer records being admitted into evidence is a 1965 Nebraska case. In this instance, the plaintiff tried to introduce into evidence a computer printout prepared by the director of accounting for the company. The director testified as to the accuracy of the printout, Bequai said, and the court allowed it to be introduced as evidence. Bequai said two Arizona State courts have also allowed local prosecutors to introduce computer printouts into evidence. On the Federal level, the Fifth and Ninth Circuits, demonstrating what Bequai termed "flexibility," had allowed computer-generated evidence into court in two cases.

Bequai went on to say, however, that while computer-generated evidence has been allowed in a few cases, in most trials such evidence has not been used. Moreover, in the trials where computer-generated evidence was involved, the courts have not been clear as to the testimony necessary to provide an adequate foundation for the admission of such evidence. "Further," Bequai said, "many courts take a very conservative position, and apply strict standards on whether to allow such evidence into court. Judges are, and rightly so, concerned about the reliability of such evidence, especially since it can easily be altered and manipulated." Bequai said that some courts have refused to allow computer-generated evidence because there was no proof that the person who prepared it had personal knowledge of the information fed into the computer. In addition, he said, "None of the courts which have dealt with these cases have handled as yet the difficult problem of laying a proper foundation to demonstrate the reliability of a computer that arrives at a complex, independently contrived conclusion."

Bequai said that litigation involving computer-generated evidence had dealt only with simple printouts. More complicated artifacts of computer technology, such as elaborate reels of magnetic tape, have been introduced in no cases; nor has an attorney sought to introduce them, Bequai said. "As computer technology advances," he said, "and records take on more elaborate and refined forms, their admissibility into court as evidence may also become more difficult. No case at present eliminates the personal knowledge requirement; nor has any case decided on whether the admission of printouts violates the confrontation or due process clause of the Constitution. The prosecution of computer criminals, at present, remains at best a difficult problem."

Bequai discussed the task of improving controls against the use of the computer in white collar crime. "The best offense in the war against computer crime is a good defense," he said, explaining that the type of defense to be deployed depended, to a large degree, on the type of system in use such as batch or integrated, inhouse terminals or remote terminals; the type of data the system handled such as confidential or secret; the principal application of the computer; and the integrity of personnel who use the computer.

Bequai offered several recommendations on how to control personnel abuse of an ADP system. Whenever possible, he said, responsibilities should be divided. He termed this concept the "separation of knowledge." Programers, for example, should not also be operators.

In addition, Bequai said, employees should be rotated so that no workers have access to any phase of the system for too long a period of time. Next, Bequai said, the system itself should be isolated from other divisions within a firm or institution. Employees in the computer system should not have access to cash and inventories. Computer personnel should not have the authority to sign checks, purchase orders, or shipping documents. Use of computer equipment should be by explicit permission only.

A record log should be kept of all system users, Bequai said, and the day and the hour they make use of the system should be logged as well. Access to the system and the data should be on a need-to-know basis only. All unexplained stoppages or interruptions should be logged and investigated as soon as possible when they occur, Bequai said.

All instructions should be in writing and not oral, Bequai said. Programers should be required to give written instructions to operators. Personnel responsibility for writing, authorizing, modifying, and running programs should be separated whenever possible. "Threat monitoring" can be built into systems with which suspicious deviations from normal patterns can be detected, Bequai said. Audit trails of changes in programs should be required. All program changes should be recorded and a reason, date, and cross-reference should be filed for each program change.

All documents sent to the computer room for input processing should be carefully accounted for; that is to say, the number sent should match the number received. Bequai said that when discrepancies surface in the numbers of documents sent to and received in the computer room then an effort should be made to reconcile the question. Any changes made on source documents for input processing should be made only by the originating department, Bequai said. All source documents should be retained for as long as possible and errors in processed data should be reported promptly to an investigative group either within or outside the firm or institution.

"Security precautions can also play an important role," Bequai said, explaining that badges or machine-readable cards should be distributed to authorized users so that the system can identify them. Such cards should be collected at the end of the day. Codes, passwords, and other verbal safeguards should be changed periodically so that even if criminals gain access to them their illicit use will be limited by the time period within which the codes are current. "Losses will thus be minimized, though not eliminated," Bequai said.

When data of a highly sensitive and secret nature is involved, scramblers and cryptographic machines should be used during the transmission of information, Bequai said. The system should record all invalid or unsuccessful attempts to enter it. For example, Bequai said, the system should be structured in such a way as to establish an audit trail of requests for files from a terminal user who is not authorized access to such files. Bequai also noted that the computer itself can be programed to disconnect terminals after a specified period of inactivity by the terminal user.

Law enforcement officials should be trained to look for certain clues which may reveal evidence of computer crime, Bequai said. Investigators should establish in their interviews with personnel whether there has been an increase in employee complaints that too much money was withheld from them in yearend earnings statements. Bequai said an upsurge in complaints like that could indicate that a violator tampered with the computer, triggering escalated withholding taxes and other payroll deductions and pocketing the proceeds himself.

Investigators should also determine if there have been customer complaints about delays in crediting their accounts with incremental payments they have made on outstanding bills. Bequai said investigators should examine computer-related documents to determine whether or not they are numbered sequentially. If purchase orders, invoices, checks, and other similar documents are not numbered sequentially, this may indicate that the ADP system has been violated in some manner, Bequai said.

He recommended that investigators make special note of the bills from a firm's time-sharing bureau. A significant increase in billings from the time-sharing bureau may reveal that the firm's own computer is being used in an unauthorized way, Bequai said. The investigator should also run a quick check of suppliers to whom payments have been made. This can easily be done, Bequai said, by calling the suppliers on the phone to make certain the suppliers do, in fact, exist. Bequai said that in the Equity Funding scandal investigators, in certain instances, had only to telephone various accounts to establish that the accounts were fake.

Bequai said:

> Various measures can be taken to minimize the vulnerability of the computer from criminal attack. Investigators can and must be trained to spot "tips" when the system is under attack. Defensive measures can also go a long way in deterring the not-so-sophisticated and organized criminal elements.
>
> However, organized crime has begun infiltrating this area, bringing with it vast resources in money and talent. At present, few computer systems, either in the private sector or government, have any well-developed defense systems to minimize criminal attacks. There are no training programs to prepare investigators and prosecutors to combat this growing problem. Further, the criminal system itself is handicapped by antiquated laws and procedures. Until some of these problems are dealt with, the computer criminal can be assured that his detection will be minimal, and his prosecution even

rarer . . . computer crime will continue to grow as a "profitable business."

PRESENT LAWS THAT MAY APPLY TO COMPUTER ABUSE

In its preliminary investigation into problems associated with computer technology in Federal programs and private industry, the staff of the Senate Government Operations Committee mistakenly assumed that the Law Enforcement Assistance Administration (LEAA) would be involved in assisting the criminal justice system in research projects aimed at strengthening the system's ability to control, detect, investigate, and prosecute computer crimes. However, LEAA is doing nothing in the computer crime field, as the following June 3, 1976, letter from LEAA Administrator Richard W. Velde to Senator Ribicoff indicated:

> DEAR MR. CHAIRMAN: This is in response to your letter of May 11, 1976, concerning the Government Operations Committee's preliminary staff inquiry into areas of computer technology.
>
> The Law Enforcement Assistance Administration has not commissioned any studies concerning illegal, questionable or irregular uses of computers in Federal programs. The reason for their being no such studies in this area is a result of LEAA's mandate to focus assistance on State and local criminal justice, rather than Federal matters.
>
> Although LEAA has sponsored several studies on white-collar crime, there have been no LEAA-sponsored studies in the area of computer illegalities and irregularities in the private sector. I have been informed that the National Science Foundation has awarded a grant to Stanford University to study computer-related crimes. Consequently, the NSF may be able to provide you with some useful information.
>
> Your interest in the programs of the Law Enforcement Assistance Administration is appreciated.
>
> Sincerely,
>
> RICHARD W. VELDE,
> *Administrator.*

The National Science Foundation sponsors computer abuse studies at the Stanford Research Institute which is located in Menlo Park, Calif., near the Stanford University campus in Palo Alto. Susan Hubbell Nycum, an attorney in San Francisco, is the principal legal consultant to the Stanford Research Institute. The SRI project is headed by Donn B. Parker. Mrs. Nycum, who has served as director of a computer center at the Carnegie-Mellon University and as director of the computer facility at Stanford University, was asked by the committee staff to provide information relating to present laws that may apply to computer abuse. The paper given the committee by Mrs. Nycum is drawn from research conducted at SRI under NSF sponsorship.

During a 4-year period ending in 1976, Stanford Research Institute's computer abuse study identified 420 cases. Donn B. Parker, who headed the project, was the leader of a team of computer experts who made an evaluation of security safeguards in the Infonet system, the largest time-sharing ADP service firm the Federal Government contracts with. The Parker study of Infonet was referred to earlier in this staff study.

In the material she submitted to the committee, Mrs. Nycum said her research in the legal aspects of computer abuse, particularly the criminal law aspects of computer abuse, demonstrated that legal sanctions can be effective deterrents to abuse. She began her presentation of her paper with a section headed "Legal Analysis" and then proceeded to cover other aspects of her research.

Mrs. Nycum's paper follows:

> *Legal analysis*
>
> The legal analysis has been an ongoing effort to study the fact patterns of the 420 cases reported to Stanford Research Institute (SRI) and to distill from the fact patterns the legal issues contained therein. Having identified the issues, I then determine what law(s), if any, have been violated by the perpetrator(s). The process of categorizing the instances of abuse for case analysis has closely followed the technical analysis that is, it is categorized by acts directed at computer hardware and to computer software systems; by acts directed to computerized assets, programs and data; by acts where the computer is itself the perpetrating device; and finally acts wherein the computer was used as a symbol, usually for harassment or intimidation.
>
> From a legal analysis standpoint, acts directed to computer hardware cause few problems. The act is a human observable occurrence, it results in a harm or loss of a standard type—deprivation of use, destruction, threatening behavior (theft, malicious mischief, extortion) and it involves a tangible object. Though sometimes bizarre (several case studies concern computer hardware actually shot at by guns), these abuses are straightforward in terms of general experience and cause little difficulty for law enforcers, prosecutors, victims, insurers, and auditors to comprehend either the extent of the loss or the method of occurrence.
>
> The acts which are directed to software but in their perpetration leave the computer hardware unscathed are, on the other hand, very difficult to detect, to pair to existing legal sanctions, and frequently to assess the extent of the damage or loss. This difficulty results from the nature of software. Software has been classified for all but State personal property and sales tax purposes, as an intangible. Though it is the complicated set of instructions which cause roomfuls of heavy equipment to run, though it causes these machines to perform useful functions in a wide variety of tasks, it can be transported across State lines invisibly and in nano-seconds (1/1,000,000,000 of a second) and copied without leaving a trace that the original had been disturbed. It can be added to, altered or deleted relatively simply by trained or ingenious persons and usually at their convenience, on site or from a

remote location. Where the software represents a confidential proprietary asset of its owner, theft of it may or may not violate State trade secret theft statutes.

State laws violated

A. *Misappropriation of software: Utilization of a remote terminal.*—When an actor utilizes a remote terminal to misappropriate software, he may run afoul of several State laws: First, the State may have misappropriation of trade secrets as a separate and distinct offense. Second, notwithstanding trade secrets laws, the actor may be guilty of larceny; as a corollary, any recipient (other than the actor) of the software would be receiving stolen goods. Third, the offender may have committed credit card fraud if he uttered a fictitious account number to obtain computer time on credit. Even if no such law is applicable, the actor may have obtained services or labor under false pretenses if he misrepresented his identity while "dumping" the software. Finally, if the offender used a telephone connection to his remote terminal, he may be guilty of fraud perpetrated by telephone.

1. *Trade secrets.*—Of the 11 jurisdictions analyzed, 4 (California, New York, New Jersey, and Texas) have statutes which make misappropriation of trade secrets separate and distinct offenses. Three (Pennsylvania, Massachusetts, and Illinois) have incorporated trade secrets into larceny statutes. The four remaining (Delaware, District of Columbia, Florida, and Virginia) have neither.

The California Trade Secrets law, California Penal Code section 499c (West 1970) proscribes four separate acts. First, section 499c(b) (1) provides that stealing, taking or carrying away an article representing a trade secret, with larcenous intent, is theft. Second, section 499c(b) (2) denominates fraudulent appropriation by a person in a position of trust (embezzlement) as theft. Third, copying a trade secret is theft, but the statute differentiates between one who has no authorized access (§ 499c(b) (3) proscribes any making of a copy at any time) and one who has, as an employee or agent (§ 499c(b) (4) proscribes copying only in the presence of the article representing the trade secret). Finally, it is a separate offense to promise, offer or give, or conspire to do the same, any inducement, bribe or reward for the divulgence of trade secrets, section 499c(c). Moreover, whoever solicits, accepts, receives or takes an inducement is guilty of this separate offense. The only obvious loophole in this otherwise comprehensive law is the employee who makes a copy of the trade secret not in the presence of the article copies, and who uses the copy himself or gives it to another without any benefit to himself.

The New York Trade Secrets law, New York Penal Law section 165.07 (McKinney 1967) is a proscription against unlawful copying of secret scientific material. Unlike California, New York separates theft of such material in the third degree larceny statute, section 155.30. A violation of section

165.07 is a class E felony, punishable by a 1 to 4 year indeterminate prison sentence, section 70, and a discretionary fine up to double the amount of any pecuniary gain from the violation, section 80. While there is no requirement for the copying to be made in the presence of the article, as in California, it is apparently no crime to cause a trade secret to be copied, as provided in California Penal Code section 499c (b)(3) and (4).

In 1965 New Jersey enacted a law whose purpose was "to clarify and restate existing law with respect to crimes involving trade secrets and to make clear that articles representing trade secrets, including the trade secrets represented thereby, constitute goods, chattels, materials and property and can be the subject of criminal acts." New Jersey Statute Annotated, section 2A:119-5.1 (1969). Section 2A:119-5.3 defines, as a separate offense from larceny, stealing, embezzling, copying, or causing to be made a copy of a trade secret. Similar to the New York statute, there is no "in the presence of the article" requirement. A violation of this section is a misdemeanor if the article is valued at less than $200, and a high misdemeanor (punishable by up to 7 years in prison and/or a fine not to exceed $2,000, 2A:85-6, 7) if the value is equal to or exceeds $200. As in California, cf. California Penal Code section 499c(d), it is no defense that the article was or was not intended to be returned, 2A:119-5.5. Curiously enough, the New Jersey statute also provides for the situation where a trade secret is taken by force, 2A:119-5.4, a high misdemeanor punishable by up to 15 years in prison and/or a fine not to exceed $5,000, *id.*

The Texas trade secrets law was added to the Texas Penal Code effective January 1, 1974. The statute, Texas Statutes Annotated, Penal Code, 31.05 (1974) proscribes stealing, copying, communicating, or transmitting a trade secret without the effective consent of the owner of the secret. A violation is a third degree felony, punishable by 2 to 10 years in prison and a fine not to exceed $5,000, 12.34. The statute is broad enough to cover any conceivable misappropriation, irrespective of asportation, privilege, or presence, and clearly extends prior case law in that it includes intangible trade secrets as protected property under 31.05(b)(3) (communication transmission) as well as tangible writings containing trade secrets. It is irrelevant that larcenous intent to deprive be present under subsections (b) (2) and (3), see S. Searcy and J. Patterson, "Practice Commentary," 31.05. Whether the broad proscription of subsection (b)(3) will survive constitutional challenge (as an infringement on free movement of ideas) is doubtful. The statute was apparently drafted in haste and added to the revised penal code without committee or bar deliberation, and has been criticized as lacking "precision, clarity, and conciseness." *Id.*

2. *Larceny.*—Larceny statutes are relevant in three different contexts. First, in States which have misappropriation of trade secrets as a separate and distinct offense, a dual

charge of larceny and theft (or abuse) of trade secrets may arise from the same act. This does not mean, however, that double punishment may be meted out when an actor engages in a single indivisible transaction which may encompass several crimes. Only the single, heaviest punishment of all the crimes may be imposed, see *Neal* v. *California*, 55 Cal. 2d 11, 19, 9 Cal. Rptr. 607, 357, P. 2d 830 (1960) (where defendant threw gasoline on two persons and ignited it, and was convicted of and sentenced on two counts of attempted murder and one count of arson, held the arson sentence was improper double punishment). See also 2 B. Witkin, California Crimes 953 (1963). The critical question is what constitutes a single indivisible transaction, cf. *People* v. *Neder*, 16 Cal. App. 3d 846, 94 Cal. Rptr. 364 (1971) (three separate fraudulent credit card transactions in one store were three separate offenses even though motivated by a unified plan to defraud the store. Second, where theft of trade secrets is subsumed into the general larceny statute, the burden of the prosecutor to prove trade secrets is property subject to larceny is eliminated. Third, even where trade secrets have not been statutorily included as property subject to larceny, the prosecutor may be able to prove that the secret is a "thing of value."

The New York larceny statute, New York Penal law § 155.30 (McKinney Supp. § 1974), is an excellent example of how a jurisdiction may include trade secrets ("secret scientific material," subd. (4)) in its larceny statute. Both stealing and copying are separate offenses, each a class E felony. If the trade secret has a readily ascertainable value (market or replacement value, see § 155.20) in excess of $1,500, the prosecutor may desire to waive prosecution under § 155.30, and instead charge under § 155.35 second degree grand larceny, a class D felony (1 to 7 years in prison and a discretionary fine similar to class E felonies).

New York appears to follow the valuation rule of *People* v. *Dolbeer*, supra n. 4 at 6. In *People* v. *Irrizari*, 5 N.Y.2d 142, 182 N.Y.S.2d 361 (1959), held the value of property stolen is what the thief would have had to pay to acquire the property. Property subject to larceny under § 155.35, which unlike § 155.30 does not specifically include secret scientific material, is "money, personal property, . . . or any article, substance or thing of value." § 155.00(1). New York Gen. Constr. Law 39 (1967) defines personal property as including intangibles as well as tangibles, and the leading judicial interpretation of "property" in New York law is "intangible property as well as tangible, . . . that is capable of being owned or transferred." *In re Bronson* 150 N.Y. 1, 44 N.E. 707, 711 (Vann, J. dissenting). Contra, *People* v. *Ashworth*, 220 App. Div. 498, 222 N.Y.S. 24 (certain intangibles cannot be the subject of larceny) and E. Marks, "Criminal Law in New York" (2d ed. 1967) § 320 (except for specifically enumerated intangibles, only tangible articles may be the subject of larceny).

Unlike New York, the California theft statute, California Penal Code § 484a (West 1970), nowhere specifically includes trade secrets as property subject to theft. While § 499c is probably the exclusive sanction for copying a trade secret without asportation, the *Ward* case indicates that a dual charge of theft (§ 484a) and theft of trade secrets (§ 499c) is maintainable where an article representing a trade secret (or a copy thereof) is asported. The *Dolbeer* case supports a dual charge. In *Dolbeer*, the court upheld a theft conviction where the res was paper containing customer lists. The court held that customer lists were property subject to theft; since customer lists are clearly trade secrets, it is no radical extension of *Dolbeer* to say that trade secrets can be the subject of theft, and their value as trade secrets is therefore added to the value of the article stolen.

A corresponding question of valuation arose in Texas under the predecessor to current Tex. Stat. Ann., Penal Code § 31.03 (1974), see *Hancock* v. *State*. Since the court held that software was property subject to larceny, there seems to be no case law prohibiting dual charges under § 31.03 and § 31.05. Cf. *Warren* v. *State* 514 S.W.2d 458 (Tex. Crim. App. 1974) ("same transaction" theory of double jeopardy rejected so long as there is separate and distinct offense). Nor is there anything in the statute itself which bars dual charges while the Practice Commentary to § 31.05 suggests that the existence of theft of trade secrets as a separate crime precludes an indictment charging multiple offenses for the same act, all § 31.02 provides is that all crimes enumerated under § 31.03 shall constitute a single offense. Sections 31.04 and 31.05 are separate offenses entirely and § 31.02's consolidation provision seems inapplicable. Thus, if the software has a readily ascertainable value greater than $10,000, the larceny becomes a second degree felony, punishable by 2 to 20 years in prison and a fine not to exceed $10,000.

It is a much closer question whether dual charges may be maintained in New Jersey. Property subject to larceny in New Jersey is limited to tangibles, certain enumerated intangibles, and anything else capable of ownership, N.J. Stat. Ann. 1:1–2 (1969). While there is some authority for reading personal property broadly to include general intangibles as well as tangibles, *see Barr* v. *Essex Trades Council*, 53 N.J. Eq. 101, 30 A. 881 (Ch. 1894) (right to do business without undue interference is protected property right at equity), a recent case held that such broad interpretations or general definitions cannot stand when they would be repugnant to the subject matter and context of the law in question. *See A&B Auto Stores* v. *City of Newark*, 103 N.J. Super. 559, 248, A.2d 258 (1968) ("property" in context of statute providing compensation of riot victims does not include intangible losses arising from business interruption, loss of profits, and good will). It is thus not clear that a *Hancock*-type case would be similarly decided in New Jersey, especially considering the fact that (1) criminal statutes are narrowly construed to benefit the defense and (2) there is an alternative sanction under 2A:119-5.3.

While New York is the only State which has incorporated trade secrets into both its own and a general larceny statute, three states—Pennsylvania, Massachusetts, and Illinois—have incorporated trade secret protection into theft or larceny statutes without denominating abuse of trade secrets as a separate offense from theft or larceny generally. Generally, trade secrets protection can be incorporated into theft or larceny statutes in three ways: first, consolidation of trade secrets into a theft or larceny statute, as in Pennsylvania; second, definition of trade secret theft as larceny, as in Massachusetts, or, third, inclusion of trade secrets in lists of property protected by larcency statutes, as in Illinois.

In 1973, Pennsylvania completely restructured its criminal code, and all theft and related offenses—such as larceny, embezzlement, false pretenses, extortion, and so forth—were consolidated into a single statutory offense: theft, Pa. Stat. Ann. title 18, section 3902 (1973). Included as one of the offenses was theft of trade secrets, section 3930 (exhibit D to App. II). Thus, although a single act—such as theft of an article containing a trade secret—could be indictable either under section 3921—theft by unlawful taking or disposition—also note that trade secrets, being intangible personal property, are property protected by section 3901—definitions—or section 3930, it could not be indictable under both. The only advantage to foregoing prosecution under section 3930 would be if the readily ascertainable value of the software was in excess of $2,000, thereby increasing the crime to a third degree felony, section 3903. Ordinarily, theft of trade secrets is a first degree misdemeanor, punishable by up to 5 years in prison and a fine of up to $10,000. Also, of interest in the Pennsylvania law is that robbery and burglary of a trade secret are denominated theft, section 3930(a); although the regular burglary statute, section 3502, provides privileged entry as a complete defense, such a defense is conspicuously lacking in section 3930. It only is a defense to a charge of theft of trade secrets that the secret was "rightfully known or available to him from a source other than the owner of the trade secret. Section 3930(d). In essence, this provision codifies the holding of the Court of Common Pleas of Chester County in *Somat Corp.* v. *Combs*, 40 D. & C. 2d 101 (1966), where the court denied equitable relief to a corporation seeking an injunction on former employees accused of misappropriating customer lists, bids, plans and layouts. Held, where such information is publicly known or available through minimal research, it is not a trade secret, nor is general knowledge and skill which may have been developed at another's expense, the same at 120.

The Massachusetts trade secrets provision was incorporated into the general larceny statute in 1967, Mass. Gen. Laws, ch. 266 30(4) (1968). Since it is clear that theft of trade secrets is not indictable under section 30(c), *see Commonwealth* v.

Engleman, 336 Mass. 12, 142, N.E. 2d 406—1957—defense motion for directed verdict of not guilty on indictment charging conspiracy to steal trade secrets should have been allowed—theft of trade secrets is clearly a single offense in Massachusetts. It seems that each State has an interesting twist to its trade secrets statutes, and Massachusetts is no exception. Section 60A of chapter 266 provides that one who knowingly receives stolen trade secrets is punishable by up to 5 years in prison or by up to 2 years in jail and a fine of not more than $500. Apparently the thief is only slightly more culpable than the recipient, since he may be fined up to $600, section 30(4). Both Pennsylvania and Massachusetts have eliminated the common law requirement of asportation—since the laws of both States proscribe copying alone—but the Massachusetts statute is more narrowly drawn than Pennsylvania's, since it is no crime to gain unlawful access to a trade secret so long as no copy is made—contrast Pa. Stat. Ann. title 18, section 3930(b)(1).

Illinois has chosen to protect trade secrets by including articles representing trade secrets as "property" protected by part C—offenses directed against property—to title III of the criminal code. Ill. Ann. Stat. Ch. 38 15–1 (Smith-Hurd 1970). Section 16–1 provides that one who, with larcenous intent, "obtains or exerts unauthorized control over property of the owner, . . ." commits theft. The phrase "obtains or exerts control" is defined in section 15–8, and includes *but is not limited to* traditional notions of asportation or deprivation (italic mine). While the italicized phrase would seem to indicate a legislative intent to eliminate the need for asportation in certain cases—such as copying a trade secret—the statute has been construed as merely restating the common law and long familiar statutory elements of larceny, *People* v. *Harden*, 42 Ill. 2d 301, 247 N.E. 2d 404, 406 (1969). While an astute judge may someday expand the definition of "obtains or exerts control" to include unauthorized exploitation without asportation, it appears now that copying or any other unauthorized use without asportation of an article representing a trade secret is not larceny in Illinois. But if one does so asport the original, he is guilty of a class 3 felony, section 16–1 (Supp. 1975), punishable by up to 10 years in prison, section 1005–8–1 (1973) and up to a $10,000 fine, section 1005–9–1, if the value of the trade secret is greater than $150.

The four remaining jurisdictions—Delaware, the District of Columbia, Florida, and Virginia—have neither a trade secrets law nor a larceny statute which incorporates trade secrets in one form or another. Each jurisdiction has either codified or retained common law larceny virtually intact, and, as a result, each provides little or no protection for theft of trade secrets or software. While each may differ slightly from the others, it can be said without much fear that first, the only property protected is tangible personal property, goods or chattels; second, the property must be asported, with third, the intent to deprive the owner permanently of use or benefit.

While Delaware, District of Columbia, and Florida include anything of value (*cf*. Dela. Code Ann. title 11 section 857(4) (1975) ("anything of value") D.C. Code section 22–2201 (1967) ("anything of value"); Fla. State Ann. section 811.021 (1) (a) (Supp. 1975) ("article of value of any kind") in their lists of property subject to larceny, it is doubtful whether this catch-all could be successfully applied at present to intangibles, see D.C. Code section 22–102 ("anything of value" defined as "... possessing intrinsic value. ..."); *United States* v. *Barlow*, 470 F.2d 1245, 1251 (D.C. Cir. 1972) (construing scope of similar phrase in theft of government property statute, 18 U.S.C. section 641); but see *Biber* v. *Miami*, 82 So. 2d 747 (Fla. 1955) (unsigned contracts, valueless in themselves, were stolen. Held, as customer lists they were articles of value and subject to larceny.) However, Bender makes a forceful argument that phrases such as "anything of value" should be broad enough to include trade secrets. The Virginia statute, Va. Code Ann. 18.1–100, 101 (Supp. 1974), covers "goods and chattels." Since larceny is a common law crime in Virginia, regulated but not defined by statute, see *Smith* v. *Cox*, 435 F. 2d 453, 457 (4th Cir. 1970), trade secrets would not be protected, *cf*. *Comment*, 24 U.Fla. L. Rev. 721 (1972) (discussion of what constitutes goods and chattels in similar provision of Florida law).

Even if trade secrets were protected property in these four jurisdictions, the clear requirement for asportation would preclude an indictment for unlawful access, copying or memorizing of a trade secret, see *Durphy* v. *United States*, 235 A.2d 326 (D.C. App. 1967) (D.C. larceny statute incorporates the common law requirement of asportation); *United States* v. *Bottone*, 365 F. 2d 389, 393 (2d Cir. 1966) (memorizing, copying or conveying do not meet the common law requirement for asportation (*dictum*), *accord*, *People* v. *Dolbeer*, 214 Cal. App. 2d 619, 29 Cal Rptr. 573, 575 (1963) (*dictum*).

The third element of the offense, intent to deprive the owner permanently of his property, is strictly construed in Florida and Virginia, see *Gaynor* v. *State*, 196 So2d 19, 21 (4th D.C.A. Fla. 1967) and *Smith* v. *Cox*, *supra*. This rigid interpretation of the *mens rea* has been softened in Delaware (see Del. Code Ann. 857(1) ("deprive" means to withhold permanently or for so extended a period as to withhold a major portion of economic value or benefit) and the District of Columbia (see *Fredericks* v. *United States*, 306 A.2d 268, 270 (D.C. App. 1973) (an intent to appropriate property to a use inconsistent with the owner's rights is sufficient to sustain a conviction under D.C. Code 22–2201); *cf*. *Pennsylvania Indemnity Fire Corp*. v. *Aldridge*, 117 F.2d 774 (D.C. App. 1941) ("theft" clause in insurance contract does not require proof of intent to deprive permanently but only proof of intent to use inconsistent with the owner's rights). The District of Columbia has also modified common law larceny to the extent that larceny may be a crime against possession and/or ownership rather than ownership alone, see *Levin* v. *United States*, 338 F.2d 265 (D.C. Cir. 1964), cert. den. 379 U.S. 999 (1965).

Delaware is the only jurisdiction in this group which may provide for criminal sanctions for theft of trade secrets, not under its larceny statute, but rather under a broad reading of its misapplication of property statute, Delaware Code Annotated 848. While the thrust of the statute is wrongful encumbrance of entrusted personal property, it is not inconceivable that an employee who misappropriates software would fall within its scope. And when the value of the property is $100 or more, the offense is a class E felony, punishable by up to 7 years in prison and/or an indeterminate fine.

Federal protection in this area

Currently the Federal forms of protection of intellectual property (patent and copyright) are not explicitly available to owners of software. The United States Supreme Court has twice in the 1970's held a particular program unpatentable. *Gottschalk* v. *Benson and Tabbott*, 93 S.Ct. 253 (1972), *Dann* v. *Johnston*, yet on neither occasion has the court held computer programs unpatentable as such.

The Copyright Office currently accepts programs for registration, but the validity and extent of the protection has yet, to my knowledge, been tested in the courts. Neither the current copyright law nor the pending legislative revision explicitly include software. The National Commission on New Technological Uses of Copyright is presently holding hearings on, inter alia, how most effectively to protect proprietary interests in software while promoting the exchange of ideas.

When the targeted asset is data stored in machine readable form (and increasingly large data bases are being created and used locally and from remote locations), the data may be proprietary and hence constitute a trade secret or a copyrightable work (see the above for a discussion of the problem of trade secret theft sanctions in a multi-State environment). The data may also contain individually identifiable personal information. As such its wrongful disclosure may be protected under Federal law (e.g., the Privacy Act of 1974 which concerns such data held by Federal agencies but not that held by nationwide corporations and other persons in the private sector) and under some State laws which affect only the public sector. (California is the only State with a currently pending bill which seeks to encompass the private sector.)

3. *Credit card abuse: theft of services or labor under false pretenses.*—While most crimes discussed in connection with software abuse have as their victim the owner of software, the computer center as well may be victimized. Since it is unlikely that an actor would use his own account number or identification code while misappropriating software, and since the computer time used in the dumping will be charged to either

the software owner or a third party (obviously without consent), the actor may be guilty of credit card theft and/or theft of services or labor under false pretenses, depending on the jurisdiction and the fact pattern. Of the 11 State jurisdictions surveyed, 9 had specific acts denominated credit card crime. Only two jurisdictions, Illinois and the District of Columbia, have no specific credit card abuse law, however both jurisdictions have theft of services laws which may be applied to credit card abuse, see Ill. Ann. Stat. Ch. 38 16-3, *Hymes* v. *United States*, 260 A. 2d 679 (D.C. App. 1970) D.C. Code 22-1301 covers credit card abuse so long as all elements of offense are proved). Beside Illinois and the District of Columbia, five States have theft of services laws (California, New York, Pennsylvania, Texas, and Delaware).

Several caveats are in order. First, in some jurisdictions, uttering a fictitious account number is enough to trigger the credit card abuse law, see, for example, Dela. Code Ann. title 11 section 904 (1975) ("credit card" includes writings, numbers, or other evidences of undertakings to pay for property). In other jurisdictions, the actor must actually utter a fictitious card; an account number system where no cards are actually issued would probably not trigger the statute, see, for example, Va. Code Ann. section 18.1-125.2(2) ("credit card" means instrument or device). Second, in States which have both credit card abuse and theft of services by false pretense statutes, dual charges may not be possible if the latter is a lesser included offense of the former. Local procedure governs. Third, theft of services and credit card abuses are statutory, not common law, larceny. The prosecutor may need to examine his jurisdiction's burglary statute (discussed more fully infra at 21-24) to see whether non-common law petit or grand larceny can trigger a burglary count charging entry of a building with intent to commit petit or grand largency, *cf. United States* v. *Frank*, 225 F.Supp. 573 (D.D.C. 1964) (intent to violate Federal Communications Act. 47 U.S.C.A. 301 *et seq.* insufficient burglarous intent to sustain prosecution under D.C. Code 22-1801 [housebreaking]).

4. *Telephone abuse.*—The actor who misappropriates software by a telephonic connection to a remote terminal may be guilty of sending a false telephone message with intent to defraud in two of the eleven jurisdictions, see Cal. Penal Code 474 (West 1970) and Ill. Ann. Stat. Ch. 134 9 (Supp. 1975). While the plain meaning of both statutes would seem to cover the case of one who uses a fictitious entry code to gain unlawful access to protected software, there may be a judicially-imposed limitation on the scope of the statute in California requiring the message to be a false relay, *see People* v. *Rand*, 23 Cal. App. 3d 579, 584, 100 Cal. Rptr. 473, 476 (1972). If such is the case, the statute would be generally inapplicable in misappropriation of software.

B. Misappropriation of software: direct access to a computation center or software storage facility.

1. Burglary. Besides those offenses previously noted, an actor who lawfully or unlawfully gains direct access to software for the purpose of misappropriating the same may additionally be guilty of burglary and/or forgery.

The California burglary statute, Cal. Penal Code section 459 (West 1970), seems applicable. First, no "breaking" is required, *see People* v. *Barry*, 94 Cal. 481, 482, 29 Pac. 1026 (1892), and privileged entry is no defense, *id*, 94 Cal. at 483, 29 Pac. at 1027. Second, a computer center may be the structure burglarized since section 459 includes buildings, and intent to commit petit or grand theft (*cf.* sections 484a, 499c, 532 and 484d—all "thefts") or any felony is the sufficient mens rea. Third, whether the offense was committed during day or nighttime is relevant only in the grading of the offense. Section 461.

The New York burglary statute is broader in some respects than California's, narrower in others, *see* N.Y. Penal Law section 140.20 (McKinney 1967). While intent to commit any crime is sufficient burglarous intent for third degree burglary, a class D felony, it is a complete defense to the charge that the actor entered upon "premises . . . open to the public . . ." unless in order to commit the crime he entered a "part of the building which is not open to the public." N.Y. Penal Law section 140.00(5).

New Jersey's burglary statute, N.J. Stat. Ann section 2A: 94–1 (1969), has (like California and New York) eliminated the necessity for breaking, covers any entry of a building with intent to steal, and disregards time of day completely. Privileged entry is no defense under New Jersey law, see 2 New Jersey Criminal Law Revision Commission, final report 235 (1971); *cf. State* v. *Young*, 57 N.J. 240, 271 A.2d 569, 577 (1970). Moreover, intent to steal may be inferred "from what transpired after the unlawful entry occurred." *State* v. *Martinez*, 112 N.J. Super, 552, 272 A.2d 289, 291 (1970).

As previously noted, Pennsylvania's theft of trade secrets law, supra at 15, has a burglary count, Pa. Stat. Ann. title 18 section 3930(a), in which privileged entry is no defense. The broader burglary statute, section 3502, does provide for such a defense, effectively limiting trade secret burglary to section 3930(a) unless the actor enters "a separately secured or occupied portion" of the computer center, section 3502(a). Intent to commit any crime is sufficient to trigger section 3502, and there is no time of day restriction.

While the Massachusetts burglary statutes, Mass. Gen. Laws ch. 266 sections 16, 16A, 17 and 18 (1968) are too narrow to cover entry without breaking (unless a person is put in fear, at night, section 17) of a computer facility, an oddball statute, ch. 266 section 20 (stealing in building) provides that one who actually steals in a building may be punished by up to 5 years in prison and a $500 fine. While there are no reported cases of dual charges under section 30 (larceny) and section 20, there seems no bar to such charges simultaneously, since section 20 describes a separate offense.

The Illinois statute, Ill. Ann. Stat. ch. 38 section 19–1 (Supp. 1975), denominates as a class 2 felony, punishable by up to 20 years in prison and a $10,000 fine any entry of a building with intent to commit a felony or theft. The offense has no requirement of time of day, nor is privileged entry of a public place a defense, nor is any breaking required, see *People* v. *Blair*, 52 Ill. 2d 371, 288 NE. 2d 443, 445 (1972) (burglary conviction of public carwash by two patrons upheld notwithstanding lack of forced entry and theft from public place).

The Texas burglary statute, Tex. Stat. Ann. Penal Code section 30.02(a) (1974), apparently allows "effective consent" as a defense. However, it is settled in Texas that a proprietor gives only a limited consent to all to enter. One who enters with an unlawful purpose does not enter with "effective consent," see *Trevino* v. *State*, 254 SW. 2d 788, 789 (Tex. Crim. App. 1952) (adopting consent theory of *People* v. *Brittain*, 142 Cal. 8, 75 P.314 (1904)). *Accord*, *Thommen* v. *State*, 505 S.W. 2d 900, 902–903 (Tex. Crim. App. 1974); see also *United States* v. *Prejean*, 494 F.2d 495, 498 n.5 (5th Cir. 1974) (limited consent doctrine of Trevino applies also to churches).

A State with a statutory defense of privileged entry similar to New York is Delaware, see Dela. Code Ann. title 11 section 829(d) (1975). The District of Columbia, D.C. Code section 22–1801 (Supp. 1970), Florida, Fla. Stat. Ann. sections 810.03, 810.05 (1969) and Virginia, Va. Code Ann. sections 18.1–88, 89 (Supp. 1974), have roughly similar burglary elements which cover entry without breaking in a building with the intent to commit a crime. While the District allows the crime to be any criminal offense not beyond the intent of Congress to be relevant, see *United States* v. *Frank*, *supra* at 21, Florida and Virginia require an intent to do something more severe (a felony in Florida and a felony or larceny at common law in Virginia). In addition, in Virginia, burglary can only be perpetrated on a building, section 18.1–88, without breaking in the nighttime.

2. Forgery.—In order to obtain access to another's software, the actor will need to discover and utilize the owner's confidential entry code, as well as his account number. The utilization of this false entry code for the purpose of defrauding or injuring any party may be forgery. While jurisdictions which have retained the common law requirements of signature and document would not be applicable, over half of the jurisdictions surveyed (California, New York, District of Columbia, Delaware, Texas and Pennsylvania) have expanded the common law scope of the crime so that any making, altering, execution, completion or authentication of any seal, signature, writing, or symbol of right, privilege or identification which may defraud or injure another is forgery.

Cal. Penal Code section 470 (West 1970) provides, inter alia, that anyone who ". . . counterfeits or forges the seal or handwriting of another . . ." is guilty of forgery. The central question is whether the entry code is either a seal or a signature. A good argument can be made which would analogize the entry code to the signature on a check (itself a form of computerized draft which utilizes OCR) or the authenticating seal of a notary or official. Moreover, in the only reported case to construe this clause, *People* v. *Burkett*, 271 Cal. App. 2d 130, 74 Cal. Rptr. 692 (1969), the court held that "seal or handwriting" was a "catch-all", broad enough to include a photocopy of a reproduction of a seal and a facsimile signature (the defendant had used photocopies of dollar bills in dollar bill changers), 271 Cal. App. 2d at 134.

The New York forgery statute, N.Y. Penal Law section 170.00 et seq. (McKinney 1967) is very comprehensive, and denominates as a class A misdemeanor false making, completion or alteration of a written instrument which may be used to advantage or disadvantage some person. Since written instruments include symbols of identification, section 170.00 (1), either a printed entry code or an account number should trigger the statute. See generally, Rothblatt, Criminal Law of New York sections 248–352.

The District of Columbia forgery law, D.C. Code section 22–1401 (1967), is a statutory, not common law, offense, see Encyclopedia Commentary section 22–1401 ¶ 3, and covers any false making of private writings which might operate to the prejudice of another.

The remaining three States, Delaware, Texas, and Pennsylvania, have similar forgery statutes, apparently patterned after the Model Penal Code section 224.1 (1965), see Historical Note, Pa. Stat. Ann. title 18 section 1401 (1973). Each includes as protected writings any symbols of "value, right, privilege or identifications". Pa. Stat. Ann. title 18 section 4101(b); Dela. Code Ann. title 11 section 863 (1975); Tex. Stat. Ann., Penal Code section 32.21(a) (2) (c). The offense is a felony in Texas and Delaware, and a misdemeanor of the first degree in Pennsylvania.

Thus, in at least 6 of the 11 jurisdictions surveyed, it is quite probable that the utilization of a false entry code, a symbol of right, privilege, and identification, which prints out on any machine, and is used to defraud or injure, is forgery. As noted in conjunction with credit card abuse and burglary, supra, the prosecutor will need to prove a fraud or injury, actual or intended, to trigger the statute. While it seems logical that any pecuniary loss should be sufficient, the prosecutor may want to charge at least one of the various theft charges applicable, since proof of value would not then be at issue.

C. Obliteration or bugging of software.—This form of abuse can be broadly characterized as criminal or malicious mischief. While all 11 States jurisdictions have criminal mischief statutes—of one type or another—which proscribe physical damage to another's personal property, 4 of 11 have, in addition, "interference with use" statutes which make it a crime to tamper or interfere with another's property so that he suffers loss.

1. Physical damage.—So long as the prosecutor successfully characterizes the damage, see discussion supra at 7, he should have no difficulty where the outward appearance of the disc or tape is unchanged. The problem of successful characterization in California should be minimized by *People* v. *Dolbeer*, *supra* at 6. California's malicious mischief statute, Cal. Penal Code section 594 (West 1970), provides that any malicious injury or destruction of personal property of another is a misdemeanor. Five other jurisdictions (Massachusetts, Mass. Gen. Laws ch. 266 section 127 (1968); Delaware, Dela. Code Ann. title 11 section 811(a) (1) (1975); the District of Columbia, D.C. Code section 22–403 (1967); Florida, Fla. Stat. Ann. section 822.18 (Supp. 1975); and Virginia, Va. Code Ann. section 18.1–172 (Supp. 1974)) have malicious or criminal mischief statutes virtually identical to California's. Penalties generally vary according to the amount of damage—except in Virginia—and large amounts of damage may give rise to felony charges in Delaware and Florida, and felony-level punishment in Massachusetts and the District of Columbia.

Unlike the jurisdictions discussed so far—which deal with tangible or personal property—New York's criminal mischief statutes use the general word "property", N.Y. Penal Law section 145.00 et seq. (McKinney 1967). But unlike the definition of property subject to theft choses in action, evidence of debt or contract, or any article, substance or thing of value, it is settled that "property" for purposes of the criminal mischief and tampering statutes means tangible property, see R. Denzer and P. McQuillan, Practice Commentary section 145.00 N.Y. Penal Law (McKinney 1967) citing *Polychrome Corp. Lithotech Corp.*, 4 App. Div. 968, 168 N.Y.S. 2d 346 (1957) (predecessor to current criminal mischief statute not intended to apply to violations of incorporeal rights). Thus, while the statute differs slightly from the California variety, the characterization problem is the same. The grading of the offense, and its punishment, vary according to the amount of damage, from fourth degree criminal mischief, section 145.00 (supp. 1975), a class A misdemeanor, to third degree, section 145.05 (supp. 1975), a class E felony, to second degree, section 145.10 (supp. 1975), a class D felony. A new offense, first degree criminal mischief, was added in 1974, section 145.12 (supp. 1975) and covers all damage by means of explosive.

The New Jersey malicious mischief statutes N.J. Stat. Ann. sections 2A:122–1 and 170–36 (1969 use differing descriptions of the *res* protected. While the former refers to personal property, the latter refers to property. In *State* v. *Shultz*, 41 N.J.L.J. 176, 177 (1917), a lower court emphasized that "in order for the offense of malicious mischief may be perpetrated, it is necessary that there be injury to property; but . . . it is not necessary that the property be entirely destroyed." The way section 2A:170–36 operates is unique among all the jurisdictions surveyed. When any malicious mischief occurs, the prosecutor charges under section 122–1, a misdemeanor. But if the defendant can prove that the value of the property damage was less than $200, see *State* v. *Tonnisen*, 92 N.J. Super. 452, 224 A. 2d 21 (1966), he cannot be convicted of a misdemeanor, but can only be adjudged a disorderly person, punishable by up to 6 months in jail and/or a fine up to $500.

Pennsylvania's criminal mischief statute is generally inapplicable, since Pennsylvania Statute Annotated, title 18, section 3304(a) (1) and (2) are limited to destruction by dangerous means or so as to cause danger to person or property. However, subsection (a)(3) seems to incorporate theft by false pretenses and extortion into criminal mischief, perhaps as a lesser included offense of theft. As such, it would be applicable where any loss was caused and the actor utilized deception to accomplish the mischief. Criminal mischief may be a summary offense, misdemeanor, or felony depending on the amount of loss, section 3304(6).

Two Texas statutes may be relevant in the case of damage to software. The Texas criminal mischief statute, Tex. Stat. Ann., Penal Code section 28.03 (1974), subsection (a)(1), provides that damage or destruction of tangible property of another is an offense. That's not unusual. However, Texas law also proscribes any alteration or destruction of a writing with intent to defraud—while the law resembles the forgery statute in its scope, it extends to any alteration irrespective of what the writing purports to be—see Tex. Stat. Ann., Penal Code section 32.47 (1974). Thus, so long as the damage is to printed software, section 32.47 would be applicable.

The Illinois criminal mischief statute, Ill. Ann. Stat. Ch. 38 section 21-1 (Smith-Hurd, 1970), is unique among all the jurisdictions in that it specifically proscribes damage to articles representing trade secrets. Section 21-1(a) provides that knowing damage to property of another is an offense. Section 15-1 defines property as "anything of value," including articles representing secret scientific information, and this definition applies to all offenses against property. The offense is punishable by up to 5 years in prison and a fine up to $500 if the value of the software damaged exceeds $150.

2. Interference with use.—Aside from the Pennsylvania statute, section 3304(a) (3), supra, which might be used in a tampering situation but does not specifically refer to interference with use as a crime, four jurisdictions have statutes which make criminal tampering a punishable offense.

Under the general rubric of criminal trespass, Cal. Penal Code section 602(j), provides that entry of lands with intent to interfere with any lawful business is a misdemeanor. New York has a broad array of antitampering statutes. N.Y. Penal Law section 145.20 (criminal tampering in the first degree, a class D felony) would be applicable to any tampering with a publicly-owned computer operation (that is, instead of Metropolitan Life, visualize a similar tampering with any public service, *cf. People* v. *Siciliano*, 40 App.

Div. 2d 818, 338 N.Y.S. 2d 478 (1972) (a public utility within the scope of section 145.20 is any furnishing of services to the public by government authority)). Section 145.15(1) (criminal tampering in the second degree, a class B misdemeanor) is a broad provision which applies to any tampering with any property which causes substantial inconvenience. It is also a class B misdemeanor to create a risk of substantial damage to property (in excess of $250), whether or not such damage occurs, section 145.25. Tex. Stat. Ann., Penal Code section 28.03(a)(2) (1974) is the Texas equivalent to the New York antitampering statute. A violation is a class C misdemeanor if the tampering caused substantial inconvenience of no ascertainable monetary amount, and a misdemeanor or felony if the amount of loss is calculable, section 28.03(b) (1)–(5). The Virginia statute, Va. Code Ann. section 18.1–183 (Supp. 1974), is similar to the California criminal trespass statute, supra, but, unlike California, specifically extends its scope to any interference "with the rights of the owner, user, or the occupant thereof . . ." As in California, the offense is a misdemeanor.

Federal sanctions

At least 40 sections of title 18 of the United States Code bear directly or indirectly on computer abuse. For ease of analysis, these are grouped into seven broad categories: (1) theft and related offenses, (2) abuse of Federal channels of communication, (3) national security offenses, (4) trespass and burglary, (5) deceptive practices, (6) malicious mischief and related offenses, and (7) miscellaneous.

A. *Theft and related offenses*

1. 18 U.S.C. section 641 (embezzlement or theft of public money, property, or records).—The basic statute which protects Federal property from theft is 18 U.S.C. section 641. The statute covers both the thief and the receiver of stolen property. While most of the terms of the statute are straightforward, several bear directly on computer abuse because of their expansive meanings.

a. One who "knowingly converts" public property violates section 641. It is no defense to a charge of unlawful conversion that one intended to return the property. *cf. Morissette* v. *United States*, 342 U.S. 246, 271–272 ("[C]onversion . . . may be consummated without any intent to keep . . ."), or made restitution, unless those acts negative the requisite mens rea. Ibid. While no court has ever considered whether one may "embezzle" or "steal" or "purloin" software, by unprivileged copying or otherwise, it is highly likely that any unprivileged abuse may be styled a "conversion."

"Conversion, however, may be consummated without any intent to keep and without any wrongful taking, where the initial possession by the converter was entirely lawful. Conversion may include misuse or abuse of property. It may reach use in an unauthorized manner . . . It is not difficult to think of intentional and knowing abuses and unauthorized uses of

Government property that might be knowing conversions but which could not be reached as embezzlement, stealing, or purloining. Knowing conversion adds significantly to the range of protection of government property . . . ." Ibid.
See also United States v. *Tijerina*, 407 F.2d 349 (10th Cir. 1969) (deprivation of control of trucks for a period of time an unlawful conversion within section 641), *cert. den.* 396 U.S. 843 (1969).

b. As broad as the notion of "conversion" is the definition of the res which is public property. The statute itself is broad enough to include theft of labor or services, *Burnett* v. *United States*, 222 F.2d 426 (6th Cir. 1955) (wrongful conversion of services and labor of two Army servicemen by Army officer), and uses the catch-all phrase "any . . . thing of value . . ."

c. The meaning of the phrase "of the United States or of any department or agency thereof" is broader than absolute ownership. An agency of the United States is, among other things, "any corporation in which the United States has a proprietary interest, . . ." 18 U.S.C. section 6; "proprietary interest" is broad enough to include any ownership of stock, *cf. United States* v. *Anderson*, 45 F. Supp. 943, 946 (S.D. Cal. 1941) (discussing predecessor to section 641), 18 U.S.C.A. & section 641 (West 1966). *Historical and Revision Notes*, at 207. It may be enough if the United States has the power to control the use of the *res*. *Bernhardt* v. *United States*, 169 F.2d 983 (6th Cir. 1948) (property under Army control at Army depot protected by section 641), even if the *res* is in private hands, *United States*, v. *Echevarria*, 262 F. Supp. 373 (D.P.R. 1967) (advances of U.S. funds paid to university are protected by section 641). And while there are cases directly on point, it seems clear that a joint interest, divided or undivided, or an equitable interest (such as a right to use) may be converted. Thus, should the government purchase the right to use certain software, and that software be misappropriated, prosecution should be available under section 641. In addition, there is a case which suggests that property in Government custody or possession, even if the Government has no legal or equitable title thereto, may be the subject of theft under a predecessor statute, *see United States* v. *Gardner*, 42 F. 829 (N.D.N.Y. 1890) (customs booty awaiting foreclosure as res subject to theft).

d. It is clear that if the software is being developed for the government, its theft or conversion violates section 641. Moreover, Anderson, *supra*, shows that raw materials may well be included under this clause, see 45 F. Supp. at 945–949.

In its broadest interpretation, any misappropriation of software which is subject to some measure of government control, custody, or ownership is a violation of section 641.

2. *18 U.S.C. 659 (theft of goods or chattels moving as, which are part of, or which constitute interstate commerce)*.—Software may be sent by interstate common carrier; when it is, section 659 protects it from theft, irrespective of ownership.

Unlike section 641, section 659 does not seem to proscribe unauthorized copying *per se* of software; while the statute utilizes "conversion," it is relevant only to the intent of the actor, and not his act, which must be embezzlement, stealing, et cetera. The only interesting question posed by section 659 is when the theft is from interstate commerce. An excellent discussion of the elements and breadth of what constitutes interstate commerce in section 659 is found in *United States* v. *Astolas*, 487 F.2d 275 (2d Cir. 1973). In rejecting appellant-defendants' claim that the trucks they hijacked were not yet (or had ceased to be) part of interstate commerce, Medina, J., quoted with approval the trial court's instruction: "The interstate character of a shipment commences at the time the property is segregated for interstate commerce and comes into possession of those who are assisting its course in interstate transportation, and continues until the property arrives at its destination and is there delivered, either by actual unloading or by being placed to be unloaded." 487 F.2d at 278. The requirement of the existence of interstate commerce relates to the time of the theft, *United States* v. *Tyers*, 487 F.2d 828 (2d Cir. 1973), so one who steals software may not pass it off later to an accomplice with the accomplice being immune, *id.* at 830. Nor is it essential that the software ownership by common carrier be protected; it is clear that section 659 covers carriage by owner, *Winer* v. *United States*, 228 F.2d 944, 947 (6th Cir. 1956), *cert. den.* 351 U.S. 906 (1956). It is equally clear that interstate commerce does end sometime, *cf.* *O'Kelley* v. *United States*, 116 F.2d 966 (8th Cir. 1941) (theft from boxcar after delivery and partial unloading), but so long as initial steps have been undertaken, *cf.* *United States* v. *Sherman*, 171 F.2d 619 (2d Cir. 1948) (labeling and delivery of bales of duck canvas to wharf), the software is en route, *cf.* *United States* v. *Maddox*, 394 F.2d 297 (4th Cir. 1968) (brief pauses in interstate journey are included within section 659), or yet to be unloaded, *O'Kelley*, *supra*, section 659 is applicable.

3. *18 U.S.C. 2314 (interstate transportation of stolen property).*—Unlike section 659, section 2314 apparently requires that the stolen property cross State lines. It does not seem sufficient merely for the stolen property to be introduced into interstate commerce. While there are no reported cases directly on point, that is, where the stolen property was delivered to an interstate carrier but did not actually cross State lines, statutory analysis in *United States* v. *Roselli*, 432 F. 2d 879, 891 (9th Cir. 1970) supports this conclusion. In *Roselli*, the court contrasted 18 U.S.C. section 1952 (antiracketeering) with section 2314, noting that use of interstate facilities or participation in interstate travel was sufficient to provide jurisdiction for the former, while failing to assert that use of interstate facilities was sufficient to trigger the latter. Moreover, reported cases involving section 2314 have all involved the crossing of State lines, see, for example,

United States v. *Sheridan*, 329 U.S. 379 (1946) (causing fraudulent check to cross State lines); *United States* v. *Hassel*, 341 F. 2d 427 (4th Cir. 1965) (causing victim of confidence game to cross State line); *United States* v. *Jacobs*, 475 F. 2d 270 (2d Cir. 1973) (causing stolen treasury bills to cross State lines); *United States* v. *Rogers*, 475 F. 2d 821 (7th Cir. 1973) (causing forged money order to cross State lines). It seems reasonable to assume that any defendant convicted under section 2314 where the goods did not cross State lines would have appealed.

A final issue raised by section 2314 is whether a copy of a program, stolen, converted or taken by fraud, and transported across State lines, can trigger section 2314. There is only one reported case of a copy used in a related prosecution, *United States* v. *Lester*, 282 F. 2d 750 (3d Cir. 1960), *cert. den.* 364 U.S. 937 (1961). In *Lester*, a co-conspirator made numerous copies of valuable geophysical maps, transported the copies across State lines, and appellant was arrested and convicted for conspiring to transport stolen maps in interstate commerce (18 U.S.C. 371). Rejecting appellant's claim that copies were not stolen property, the court held that the property stolen was the valuable idea, not the paper embodiment. 282 F. 2d at 755. Although the court in *Lester* found no need to elaborate upon its holding, it could have cited *United States* v. *Handler*, 142 F. 2d 351 (2d Cir. 1944), *cert. den.* 323 U.S. 741 (1944), the most thorough analysis to date of what is stolen property. After analyzing other case law, the meaning of "stealing", and the legislative history of the National Stolen Property Act, now section 2314, the court concluded: (1) the stolen property need not be taken larcenously, that is, there are no requirements such as asportation, tangibility, et cetera; and (2) "the statute is applicable to any taken whereby a person dishonestly obtains goods or securities belonging to another with the intent to deprive the owner of the rights and benefit of ownership." 142 F. 2d at 353. Since a copy of a program will indeed deprive the rightful owner of the benefits of ownership, a copying should create the stolen property necessary to trigger section 2314.

4. *18 U.S.C. 661* (*theft within special maritime and territorial jurisdiction*). When software is stolen in a Federal enclave, as defined by 18 U.S.C. 7 (*see* discussion *supra* at 2–3), a violation of section 661 occurs. As in sections 641 and 2314, the question again arises whether unauthorized copying is a violation of the statute. While it was assumed (for analytical purposes) earlier in this memorandum that copying is not within the scope of section 661, a broad reading of the statute may well include copying. In *United States* v. *Henry*, 447 F.2d 283 (3d Cir. 1971), appellant was convicted for stealing a boat within the maritime jurisdiction. On appeal, it was argued that the statute was merely a codification of common law larceny, and since the Government failed to offer proof that appellant intended to permanently deprive the owner of

his property, the conviction should be overturned. In rejecting appellant's claim, the court held that the statute was broader than common law larceny. Drawing on the Second Circuit's definition of "to steal" in *Handler*, *supra*, the court concluded that when one "willfully obtains or retains possession of property belonging to another without the permission or beyond any permission given with the intent to deprive the owner of the benefit of ownership," 447 F.2d at 286, an offense was made out under section 661. As noted earlier, the "deprivation of benefit" theory should enable a prosecutor to support an indictment for unauthorized copying.

5. *Miscellaneous theft and theft-related offenses.*

(a) Theft of labor, services, or property under false pretenses. While there is no general Federal statute prohibiting theft by false pretenses, courts have construed 18 U.S.C. 641 (theft of public property) to include false pretenses, *see Burnett* v. *United States*, *supra; Morgan* v. *United States*, 380 F.2d 686 (9th Cir. 1967) (tax fraud as theft of Government money by false pretenses). Thus, there seems no bar to charging one who fraudulently obtains computer time from the United States (while stealing software) with a violation of section 641.

(b) Receiving stolen property. Many theft statutes, *see, e.g.*, 18 U.S.C. 641, 659, and 2314, *supra*, have receiving stolen property provisions as well. In addition, 18 U.S.C. 662 prohibits receiving stolen property within the special maritime and territorial jurisdiction. Section 2315 proscribes the reception of goods stolen from interstate commerce. Thus, not only may one who induces the theft of software be charged as a principal, 18 U.S.C. 2, or as a conspirator, 18 U.S.C. 371, he may also run afoul of the foregoing section.

c. There are numerous Federal statutes designed to cover specific types of theft, but which may be applicable to certain instances of software abuse. For instance, if one has the misfortune to steal a program used in the payment of Government money, he violates 18 U.S.C. section 285 (taking or using papers relating to claims). If a Government employee wrongfully converts, cf. *Morissette*, supra, the property of another which is entrusted to him, he commits an offense under 18 U.S.C. section 654. This section would be particularly effective when the employee provided a copy to an unauthorized third party. Theft of programs from federally insured banks and financial institutions is covered by 18 U.S.C. sections 655–657, although I have some doubt as to whether nonmonetary property is covered by section 656, since the protected res is "moneys, funds, or credits," in contrast to "other property of value," section 655, and "other things of value," section 657. But this loophole is closed by 18 U.S.C. section 2113(b) which covers the theft of "any property . . . or any other thing of value . . ." from a bank or savings institution. And finally, if the thief "steals, purloins, or embezzles" property "used" by the Postal Service, he violates section 1707.

B. *Abuse of Federal channels of communication*

1. *18 U.S.C. 1341 (mail fraud)*. The mail fraud statute has two essential elements: (1) one must use the mail for the purpose of executing, or attempting to execute, (2) a fraud or a scheme to obtain money or property under false pretenses. The courts have been generous in their definition of what is a fraud. The classic statement by Judge Holmes, "[t]he law does not define fraud; it needs no definition; it is as old as falsehood and as versable as human ingenuity." *Weiss* v. *United States*, 122 F.2d 675, 681 (5th Cir. 1941), cert. den. 314 U.S. 687 (1941) (construing scope of fraud in predecessor to section 1341) was quoted with approval in *Blackly* v. *United States*, 380 F.2d 665 (5th Cir. 1967) (referral selling plan as fraud) and *United States* v. *States*, 362 F. Supp. 1293 (E.D. Mo. 1973) (ballot box fraud in primary election as mail fraud), aff'd 488 F.2d 761 (8th Cir. 1973) (see cases cited therein), cert. den. 417 U.S. 909, 417 U.S. 950 (1974). Thus, the thrust of the various court opinions would include any scheme to copy software as a scheme would trigger the statute. If the thief uses a mailing to defraud a computer center (services, labor, credit, etc.), *United States* v. *Owen*, 492 F.2d 1100 (5th Cir. 1974) (mailings which led to receipt of goods on credit as mail fraud), or uses a mailing to obtain the software itself (property), he falls within the scope of section 1341. Because of the breadth of section 1341, the prosecutor should always explore its applicability in any instance of computer abuse. For a prosecutor's opinion of the effectiveness of section 1341 (and, in contrast, the ineffectiveness of the proposed Code), see Givens, "The Proposed New Federal Criminal Code," 43 N.Y. St. B.J. 486, 488–494 (1971) passim.

2. *18 U.S.C. 1343 (wire fraud)*. The elements of section 1343 are identical to section 1341, with the exception of the Federal medium abused. When one uses a remote terminal to perpetrate a computer fraud, or when one telephones an accomplice, so long as the message crosses State lines, the statute is applicable. While one commentator, see Levine, supra, at 30, has noted that the Proposed Code would cover intra- or interstate calls because of the facilities used, cf. *Final Report* section 201(e), all reported cases involving section 1343 have dealt with conversations which crossed State lines, leading me to believe that, if Levine is correct, the Proposed Code expands present jurisdiction. Since section 1343, unlike the Proposed Code section 201(e), does not use the word "facility," jurisdiction hinges on use of an interstate wire, notwithstanding the fact that "[I]t cannot be questioned that the Nation's vast network of telephone lines constitutes interstate commerce." *United States* v. *Holder*, 302 F. Supp. 296, 298 (D. Mont. 1969). Despite Levine, *supra*, it is not clear that the Proposed Code will embrace intrastate calls, either, see *United States* v. *DeSapio*, 299 F. Supp. 436, 448 (S.D.N.Y. 1969) (construing phrase "facility in . . . interstate commerce" as requiring interstate calls for 18 U.S.C. section

1952), since there may be a distinct difference between facilities "in" interstate commerce and facilities "of" interstate commerce. Ibid., cf. 15 U.S.C. section 78j (Securities Exchange Act).

C. *National security offenses*

1. *18 U.S.C. 793 (gathering, transmitting, or losing defense information)*.—This section, as well as those which follow in this category, are of limited use in software abuse. But, as a general rule, whenever abuse involves classified, restricted, or defense software, these sections should be inspected for applicability. Section 793 is broad in scope; subsection (a), the geographical intrusion provision, covers property owned, controlled, or used by contractors of the Government when the property is related to or connected with national defense. The section also proscribes copying of defense information, unlawful reception, communication of contents, and grossly negligent loss. The statute has been sufficiently definite to satisfy due process requirements, *Gorin* v. *United States*, 312 U.S. 19 (1941), and has been held to encompass "related activities of national defense" as well as military enclaves, *id.* at 28. See also *United States* v. *Drummond*, 354 F.2d 132, 151 (2d Cir. 1965) (upholding jury charge in same language).

2. *18 U.S.C. 794 (gathering or delivering defense information to aid foreign government)*.—This statute provides more severe penalties for actual transmission of the defense information to a foreign government, and also includes a conspiracy count. One caveat should be mentioned in any discussion of sections 793 or 794, or companion statute section 798 (disclosure of classified information). While it has always been true that public information is outside the scope of the protected res, see *Gorin*, supra, at 28; see also *United States* v. *Heine*, 151 F. 2d 813 (2d Cir. 1945) (officially disseminated information, no matter how painstakingly culled and digested, is not "defense information"), the Pentagon Papers case, *New York Times Co.* v. *United States*, 403 U.S. 713 (1971), now makes it clear that mere classification is not enough. The flavor of the Black, Douglas, Brennan, and Marshall opinions is that, even in criminal prosecutions, lack of substantial injury to national security might be a valid defense. While it is true that White and Stewart sharply contrasted civil injunctive (unpermitted) and criminal (permitted) sanctions, *id.* at 727–740, there is language in the Stewart opinion which hints at a need for narrowly construed guidelines on classification, id. at 729. Thus, a clear majority in the case would seem to support the proposition that classified material which had no business being classified (such as information relating to Department of Defense lobbying efforts) could not support a prosecution under chapter 37 of title 18.

3. *18 U.S.C. 795 (photographing and sketching defense installations)*.—In 1950, President Truman declared, pursuant to section 795, that all military and commercial defense establishments were to be protected against unauthorized photographing and sketching, Executive Order 10104, 15 Federal

Regulation 597, 598 (1950). Since the statute covers "graphical representations" of classified "equipment," it is probable that copying classified software would fall within this section.

4. *18 U.S.C. 797 (publication and sale of photographs)*.—18 U.S.C. 797 deals with subsequent publication and sale of photographs or sketches of equipment denominated in section 795. Section 798, which deals with codes and cryptographic systems, would be pertinent in any abuse from agencies involved in communications work. Section 799 deals with security violations of NASA regulations and section 952 deals with disclosure of diplomatic codes.

D. *Trespass and burglary.*

1. *Criminal trespass.*—There is no general Federal statute covering criminal trespass. In fact, the only statute which denominates trespass a crime in title 18 is section 2152 (trespass on fortifications or harbor-defense areas). Section 2278a of title 42 forbids trespass on installations of the Atomic Energy Commission. Neither is particularly applicable to trespass for the purpose of misappropriating software, unless the situs of the trespass is a fortification, harbor-defense area, or AEC installation.

2. *Burglary.*—The Federal burglary statutes are a bit more comprehensive, but not much. Title 18 provides criminal penalties for burglary of a bank, section 2113(a), post offices, section 2115, and interstate carrier facilities, section 2117.

a. *18 U.S.C. 2113(a)*.—While some States have denominated copying of trade secrets as larceny, it seems doubtful that entry of a bank to copy software would make out a Federal crime, notwithstanding the language "or any larceny" of section 2113(a), *United States* v. *Rogers*, 289 F. 2d 433, 437 4th Cir. 1961) (the language of the statute refers only to common law larceny). The Supreme Court has rejected a claim that Federal criminal law in this case turns on State law, *Jerome* v. *United States*, 318 U.S. 101, 106 (1943) (State felonies irrelevant). Once beyond those restrictions, however, the statute is effective against most traditional defenses. Privileged entry is no defense, see *Audett* v. *United States*, 132 F.2d 528, 529 (8th Cir. 1942) (entry may include "walking in [with] a stream of customers through the front door . . . in business hours"), nor is breaking an element of the offense. Although burglary statutes were originally designed to protect occupied spaces from crime, occupancy is irrelevant for purposes of section 2113(a), *United States* v. *Poindexter*, 293 F. 2d 329 (6th Cir. 1961), cert. den. 368 U.S. 961 (1962).

b. *18 U.S.C. 2115*.—Unlike section 2113(a), section 2115 requires forcible breaking as an element of the offense. The only vague term in the statute is "depredation." While the parameters of the term are fuzzy, depredation is generally held to mean plundering, robbing, or pillaging, see *Deal* v. *United States*, 274 U.S. 277, 283 (1927) (construing similar language in postal regulations).

c. *18 U.S.C. 2117.*—Similar to section 2115, this section, prohibiting burglary of interstate carrier facilities, also requires a breaking. Again, mens rea is "intent to commit larceny," which would be common law larceny, cf. *Rogers*, supra.

E. *Deceptive practices.*

1. *18 U.S.C. 912* (*obtaining thing of value by impersonating officer or employee of the United States*).—It may often be the case that one who misappropriates software within a federally protected sphere has falsely represented himself as a Government officer or employee in order to gain access to the software. In such a case, a violation of section 912 will have occurred. There is no requirement that the "thing of value" be tangible, cf. *United States* v. *Lepowitch*, 318 U.S. 702 (1943) (fraudulent acquisition of information about whereabouts of another), and a copy of the software would certainly seem to fall within the definition. The statute must be read broadly to encompass new concepts of "thing of value," for "[I]t was not possible for Congress in enacting the statute to anticipate all the devices and schemes which human knavery might conceive in securing benefits. . . ." *United States* v. *Ballard*, 118 F. 757 (D. Mo. 1902) (meals and lodging are a thing of value).

2. *18 U.S.C. 1001.*—When one places section 1001, the catchall which deals with all manner of false representations, next to section 912, supra, one notices that the general statute carries a much more severe penalty than the specific statute. In addition, section 1001 requires no fraudulent obtaining of a thing of value; a false, fictitious or fradulent statement (knowingly and willfully made) is enough to trigger the statute. Whatever one may say about the jurisprudential wisdom of the statute, it seems directly applicable to almost every instance of computer abuse in the Federal sphere. For example, software may not be divulged to unauthorized persons, cf. 5 U.S.C. 552(b)(4) (trade secrets subsection of Freedom of Information Act). Therefore, one who fails to identify himself as unauthorized conceals a material fact, whether or not he represents himself as authorized (is active misrepresentation a less serious crime? Cf. 912). Moreover, this section applies to both oral and written misrepresentations, see *United States* v. *Zavala*, 139 F.2d 830 (2d Cir. 1944) (false oral and written customs declaration). It may even be applicable to electronic impulses from a remote terminal which falsely represent the sender as one authorized access to protected software.

3. *18 U.S.C. 1005, 1006* (*false entries in records of banks and credit institutions*).—Whenever anyone makes a false entry in a bank or credit institution record, with intent to injure or defraud, he runs afoul of section 1005 or section 1006. While both statutes are quite fact specific, they are comprehensive in their respective areas. Since the purpose of the statutes was to insure correctness of bank records, *United*

States v. *Giles*, 300 U.S. 41, 48, active or passive omissions or commissions are covered, ibid. (teller's failure to file deposit slips is equivalent to making of a false entry). Considering the purpose noted in Giles, the breadth with which "bank books" has been interpreted, cf. *Lewis* v. *United States*, 22 F.2d 760 (8th Cir. 1927) (minutes of meetings of board of directors were "bank books"), and the need to protect banks, from loss, *Weir* v. *United States*, 92 F.2d 634 (7th Cir. 1937), it seems reasonable that computer records should be within the scope of sections 1005 and 1006; thus, any false entry, obliteration, or alteration or computerized bank records would be a violation of either section 1005 or 1006.

F. *Property destruction.*

1. *18 U.S.C. 81* (*arson within special maritime and territorial jurisdiction*).—While arson may be only infrequently used as a tactic in computer abuse, the prosecutor should be aware of the scope of the statute. The key question is whether hardware or software may be included within the phrase "machinery or building materials or supplies." A recent case arising from the Wounded Knee occupation indicates that the definition of the phrase may be narrowly construed. In *United States* v. *Banks*, 368 F. Supp. 1245 (D. S.D. 1973), the defendant-appellant was accused and convicted of violating section 81 by burning motor vehicles within a Federal enclave. Holding that motor vehicles were not "machinery" within section 81, the court Nichol, J., invoked ejusdem generis and noted that a broad interpretation of "machinery" would endanger the statute as too vague, lacking the "requirement of definiteness . . . that a person of ordinary intelligence must be given fair notice that his contemplated conduct is forbidden. . . ." 368 F. Supp. at 1248. Thus, a prosecutor might be advised to style any indictment alleging the burning of hardware (or software) as, alternatively, an attempt to set fire to a building or structure.

2. *18 U.S.C. 1361* (*malicious injury to Government property*).—While the general problem areas associated with "characterization" in cases of malicious mischief were explored in the previous memorandum (that is, what is injury, what is property), several cases construing section 1361 demonstrate the liberality with which various courts have accepted indictments charging injury. Section 1361 was somewhat of a dead letter until interference with the selective service began to mushroom in the 1960's. It was resurrected as a "catchall" to encompass otherwise unindictable offenses. For instance, in *United States* v. *Eberhardt*, 417 F. 2d 1009 (4th Cir. 1969), the Fourth Circuit considered the famous Baltimore blood-pouring case. Father Philip Berrigan and two others were convicted of violating section 1361 in that they poured blood on selective service records. In affirming the convictions, the court utilized the cost of restoring the records as the measure of damage. The appellants did not argue that blood pouring was not "injury" within the mean-

ing of the statute. As a result, the breadth of the case is not clear. At its narrowest, it would mean that any temporary physical obliteration, subsequently restored, is an "injury." At its broadest, it would support an "interference with use" theory of "injury." While the res in most selective service cases was Government records at least arguably critical to national defense, other cases construing section 1361 show that neither the injury, nor the res injured, need be terribly major, see for example *Tillman* v. *United States*, 406 F. 2d 930 (5th Cir. 1969) (glass door at induction station broken by draft resisters); *Edwards* v. *United States*, 361 F. 2d 732 (8th Cir. 1966) (removal of plumbing fixture from vacant home); *Brunette* v. *United States*, 378 F. 2d 18 (9th Cir. 1967) (dented fender). Putting these cases together with the broadest holding of Eberhardt may enable a prosecutor to argue successfully that an interference with the use of Government software is "injury," and the measure of damage is either the cost of restoration or the cost of development (if not restorable).

3. *18 U.S.C. 1363* (*malicious injury within the special maritime and territorial jurisdiction*).—This section differs from section 81, supra, only in its substitution of malicious mischief for arson.

4. *18 U.S.C. 2071* (*concealment, removal, or mutilation of public records*).—Another statute which was resurrected during the Vietnam-protest era, section 2071 should be effective against misappropriation of computerized government records, especially when a traditional larceny charge cannot be sustained (e.g. copying via a remote terminal without subsequent asportation). The bulk of section 2071 cases deal with Selective Service records and documents, see, e.g. *Eberhardt*, supra, *United States* v. *Chase*, 309 F. Supp. 430 (N.D. Ill. 1970); *Chase* v. *United States*, 468 F.2d 141 (7th Cir. 1972); *United States* v. *Donner*, 497 F.2d 184 (7th Cir. 1974), and thus it would be extending case law to include computerized records as a "document or other thing." Nonetheless, such an extension is rational. The purpose of section 2071 "is to prevent any conduct which deprives the Government of the use of its documents, be it by concealing, destruction, or removal." *United States* v. *Rosner*, 352 F. Supp. 919 (S.D.N.Y. 1972). The res, protected by section 2071 is not merely documentary or written records, but any type of public record, c.f. *United States* v. *De Groat*, 30 F. 764 (E.D. Mich. 1887) (emphasizing the thrust of the statute as toward records, not papers). And under Bauman, J.'s, analysis in *Rosner*, dumping or obliterating a computerized record surely deprives the Government of its use as much as a blood-pouring, Eberhardt, supra, or a burning, Chase, supra, or a mutilation, Donner, supra.

5. *Destruction of property affecting national security.*

a. 18 U.S.C. 2153 (willful injury to war or national defense material during war on national emergency). The extreme breadth of what constitutes the protected res in section 2153 can be seen in its definition in section 2151. War material includes "all articles, parts or ingredients, intended for, adopted to, or suitable for . . . the conduct of war or defense activities." Since the mind has trouble visualizing what in the computer industry would not fall within the definition, it seems clear that (so long as scienter is proved) hardware and software within the "defense" orbit are protected. Although the statute applies only during war or national emergency, the national emergency declared by President Truman on December 16, 1950, Proc. 2912, apparently still exists *United States* v. *Achtenberg*, 459 F. 2d 91 (8th Cir. 1972), cert. den. 409 U.S. 932 (1972).

b. 18 U.S.C. 2155 (willful injury to national defense material). The only substantive difference from section 2153 is this section's applicability irrespective of war or national emergency.

6. *Tampering.*—While section 1361, supra, may be construed to reach certain interferences with use, at present there is no generally applicable interference with use or "tampering" statute in the Code. The Proposed Code would be a distinct improvement over the present Code, in that it would make physical obstruction of a Government function, final report section 1301, and tampering with a public service, final report section 1706, criminal acts.

G. *Miscellaneous Provisions.*

1. *Derivative crimes and conspiracy.*

a. Acts which become criminal only because of the criminal acts of another, or derivative crimes, are covered in 18 U.S.C. section 2 (aiding and abetting) and section 3 (accessory). As a general rule, any action prior to the crime which induces the criminal act exposes the one who induces to punishment as a principal. Any action subsequent to the crime in the nature of assistance exposes the assistant to a charge of accessory after the fact. Thus, a third party who induces a theft of software, while not indictable by section 641, is indictable under section 2.

b. 18 U.S.C. 371 (conspiracy). While there is no general statute which makes it a crime to defraud the government, see final report, section 1004, comment at 71, it is a crime for two or more persons to conspire to (commit any offense or) defraud the United States. This leads to an anomaly: the planning of an act, not criminal in itself, may be a crime. The implications for software abuse are enormous. The broad scope of what it means to "defraud" the United States can be seen in the leading case in this area, *Haas* v. *Henkel*, 216 U.S. 462 (1910). In Haas, three persons (one of whom was a statistician with the Department of Agriculture) conspired to falsify official reports concerning cotton crops and to divulge confidential information concerning those crops to unauthorized persons in order that they might speculate in the cotton market. While there was no allegation of pecuniary loss to the

Government, the court rejected a motion to quash the indictment in a habeas corpus proceeding, holding:

> " . . . it is not essential that such a conspiracy shall contemplate a financial loss or that one shall result. The statute is broad enough in its terms to include any conspiracy for the purpose of impairing, obstructing, or defeating the lawful function of any department of Government. . . . [I]t must follow that any conspiracy which is calculated to obstruct or impair its efficiency and destroy the value of its operations . . . would be to defraud the United States by depriving it of its lawful right and duty of promulgating or diffusing information. . . ."

216 U.S. at 479–480. *Accord, United States* v. *Johnson*, 383 U.S. 169, 172 (1966) (conspiracy by two Congressmen to influence Justice Department). A minor and somewhat redundant (in light of the gloss *Haas* puts section 371) conspiracy statute is 18 U.S.C. section 286 (conspiracy to defraud by payment or allowance of false claims).

2. *18 U.S.C. 1905 (disclosure of confidential information).*—This section is potentially applicable to computer abuse in two types of situations: (a) where a Government officer or employee discloses or communicates the contents of software in Government custody but owned by private person; and (b) same as (a), but where the Government owns the software.

a. *Disclosure of "custodial" software.*—Obviously the trades secrets of section 1905, makes such an act illegal unless the disclosure is "authorized by law." The only law presently requiring wholesale disclosure of information is the Freedom of Information Act, 5 U.S.C. 552, 81 Stat. 56 (1967); however, the act does not apply to disclosure of matters which are trade secrets, 5 U.S.C. 552(b) (4).

b. *Disclosure of Government software.*—It appears that if the Government develops its own programs, such programs must be divulged on demand unless they are classified, section 552(b) (1) or a trade secret. In reality, agencies have been loath to divulge their staff-prepared programs, see Comment, "Public Access to Government-Held Computer Information," 68 NW. L. Rev. 433, 452 (1973). Whether this reluctance is enough to make them trade secrets is doubtful, see *Schapiro* v. *S.E.C.*, 339 F. Supp. 467 (D. D.C. 1972) (staff-prepared report on offboard stock trading not "trade secret" within section 552 and not prevented from disclosure by section 1905). Indeed, under the Norwegian Nitrogen Products definition, it seems hard to imagine the Government having its own trade secret, unless it is engaged in a marketing operation. Thus, it seems that any disclosure made pursuant to a section 552 request would exempt the actor from section 1905 liability. For practical purposes, all Government software which can be classified, should be classified for that reason.

Electronic funds transfer systems

Another current problem area in the Federal law is electronic funds transfer systems (EFTS). EFTS is presently under study by the Electronic Funds Transfer Commission. While the Commission no doubt will address problems of computer abuse, it is not redundant to point out one of the very real legal problems with security of EFTS is concern with the financial transaction performed other than totally within a bank or thrift institution (banks). Financial transactions resulting in a debit of a customer's bank account and a credit to a merchant's account may take place at a merchant establishment miles from the bank. Yet consider the current legal protection for banks as stated by Stephen M. Ege "Electronic Funds Transfer: A Survey of Problems and Prospects in 1975," 35 Maryland Law Review 1 (1975).

"Literature already discusses some of the varieties of criminality that the introduction of electronic data processing affords. There are at least four areas where the intervention of protective criminal law sanctions will be appropriate: (1) unauthorized access to a customer's account by means of the theft or reproduction of an access "key," such as the plastic card, given the customer; (2) unauthorized access to accounts by personnel manning access terminals, such as the store employees operating the supermarket remote deposit-withdrawal system; (3) unauthorized access to communication lines between remote terminals and information storage areas, such as a financial institution's central processing unit (in short, wiretapping); and (4) unauthorized access at the central processing unit site by employees or outsiders.

"The Federal Consumer Credit Protection Act currently makes criminal the use of 'any counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained credit card.' This prohibition, however, contemplates the use of an instrument to obtain goods or services on credit and not the use of an instrument in a transaction which is regarded as effecting a payment, or a deposit or withdrawal, from an account maintained at a financial instituiton. A similar prohibition applicable to noncredit transactions may be necessary.

"For operators of EFT terminals it will be important to decide whether they are 'in' or 'out' of the bank system for purposes of the application of Federal criminal sanctions against those who trifle with federally regulated financial institutions, since Federal law distinguishes between 'insiders' and 'outsiders.' Sections 656 and 657 of title 18, for example, make theft, embezzlement, and the like criminal where the perpetrator is an officer, employee, or is 'an . . . agent . . . of, or connected in any capacity' with federally regulated banks and savings and loan associations. This 'insider provision' has been held to reach an employee of a corporation in which a bank has an equity interest. Cases defining 'money,' 'funds,' and 'credits' for purposes of insider crime will probably require revisitation in attempting to apply the sanctions of these two sections to EFT systems. It may be supposed that these provisions apply as well to malefactions at the point of information storage, which may be, but need not be, at a financial institution's central processing unit. By parity of reasoning, 'distributed information' systems, involving storage of information at locations remote from the central processing unit, would seemingly likewise find the protection of these provisions.

"As an example of outside crime, the bank robbery statute, which applies to federally regulated banks, savings and loan associations, and credit unions, applies to whoever forceably takes or takes with intent to steal—property, money, or anything of value of the specified financial institutions. It seems, then, that where outsiders are involved it will only be necessary to find the 'tak[ing] . . . [of] any . . . thing of value,' but for insiders the required connection with the bank or savings and loan association will have to be shown.

"Interception of communications between points in the system, such as between the point of purchase and the central processing unit, or the unauthorized entry of information between points might come within the ambit of protections afforded by title III of the Omnibus Crime Control and Safe Streets Act of 1968, although by indirection. One of the purposes of this legislation is to protect the privacy of wire and oral communications. Section 2511(1)(a) makes it a Federal crime to willfully intercept any wire or oral communication. 'Intercept' is defined, in relevant part, as the '*aural* acquisition of the contents of any wire . . . communication through the use of any electronic, mechanical or other device.' Since identifying and authorizing information will not be transmitted in a form understandable to the human ear, it is questionable whether this prohibition on 'aural' acquisition can be overcome, even assuming only the 'privacy' of communications and not their unauthorized use or entry is all that need be protected.* By analogy the criminal sanctions imposed by sections 656, 657, and 2113 could, perhaps, be applied to interceptions of wire communications with intent to commit larceny, and the like, rather than placing reliance upon the Safe Streets Act, which looks to the protection of privacy rather than to the protection of the integrity of financial institution operations (for insiders) and the property entrusted to them (from unlawful access by outsiders)."

DEPARTMENT OF JUSTICE

Senator Ribicoff asked Richard L. Thornburgh, Assistant Attorney Attorney General for the Criminal Division of the Justice Department, to respond to the issue of computer crime and computer

---

*H.B. 214 would delete "aural" from section 2511(1)(a).

technology. On November 15, 1976, Assistant Attorney General Thornburgh submitted this statement to the committee:

> I am pleased to present the views of the Department of Justice on the subject of computer-related crime. While I recognize that any discussion of this kind profits greatly from concrete examples, we must be aware that in the computer crime area, many of the more instructive cases are presently in various stages of investigation or prosecution. Therefore, I will try to be as specific as possible without at the same time compromising any ongoing legal proceedings at the Federal or State level.
>
> Investigations carried out by the General Accounting Office (GAO) confirm what many have suspected—that computers may well be out of control. This statement is certainly an overly broad generalization. But if we abandon the notion that computers are superhuman robots—the idea that the computer is a mystical panacea for the shortcoming of mortals—and accept the plain fact that computers require the constant supervision of human beings, we can take a giant step toward properly addressing the problem of computer abuse.
>
> Even as a layman without any specific training in the machinations of the computer, I was not surprised by the GAO revelations.
>
> If it takes a publisher's computer months to acknowledge the change of address on my magazine subscription, I can imagine how long it will take an inventory control computer to acknowledge the disappearance of merchandise from some far-flung regional warehouse. If we are billed for merchandise we never bought, it is not unreasonable to conclude that someone may be "buying" merchandise for which they are never billed.
>
> If in its first 27 months of operation, the Social Security Administration's new Federal welfare computer will have permitted some $620 million in apparently negligent overpayments—as a recent HEW audit revealed—have we not created an irresistible temptation for fraud?
>
> Out of the ill-designed programs, the lax supervision and the human negligence that we loosely label "computer error," we may well have in fact, created not only the perfect climate for new types of crime but a convenient fallguy—the computer—as well. Thus, we must take a closer look at this phenomenon.
>
> For purposes of discussion, I suggest we divide computer crime into three broad categories: The computer as victim, the computer as an environment for crime, and the computer as accomplice.
>
> First, there are those situations where the computer itself is a victim. The computer may be the physical target of the arsonist, the vandal, the extortionist. These are traditional crimes; their investigation and prosecution evoke a traditional response from law enforcement. But for the computer user and the Government policymaker, computer-targeted crime

raises novel questions. By continuing to concentrate information and decisionmaking in centralized data systems, are we overexposing society to the threats of the extortionist, or the intimidation of the vandal?

It is estimated, for example, that 60 percent of the banks in this country could not open for business tomorrow if the computer processing their demand deposits failed them tonight. As we come to rely increasingly on the computer to perform the basic functions of society—as we move into the era of electronic fund transfer, computerized stock exchanges, and central data banks—we increase our vulnerability. We must recognize this vulnerability and be prepared to protect ourselves.

Second, there are those cases where the computer provides a conducive environment for crime. An excellent example is the culprit who walked into his bank, picked up a handful of blank deposit slips, returned to his office and encoded the slips with his own account number using his firm's magnetic typewriter. Later, he replaced the altered deposit slips on the bank's counter. Unwittingly, other customers used the altered slips to make their deposits. All the deposits for the day mysteriously end up in the culprit's account. He needed no great knowledge of computers but he did know one thing—if there was a magnetic number anywhere on the deposit slip the computer would ignore the legitimate handwritten number. The next day he could close his account and vanish with $50,000. In a similar vein, a number of the crimes identified in the GAO study involve clerks who simply enter fraudulent payment vouchers in a computer system realizing any payment below a certain amount would never be subject to human verification. In both these examples, the computer criminal was not a computer scientist; he had no specialized training; he simply had the necessary limited knowledge about the system that enabled him to pinpoint its vulnerability.

In other cases which fall into this second category, the computer becomes an accessory after the fact. The principals in the Equity Funding case perpetrated a traditional stock and insurance fraud, but they used the computer and its reams of printouts to impress their investors, "snow" their auditors, and keep investigators off their trail.

The computer has even been offered as an alibi; in an enforcement action by the FTC, a major retailer argued—albeit unsuccessfully—that its computer design made it impossible to provide the disclosures required by "truth-in-lending" laws and regulations. In some instances, it is the absence of the computer that may constitute the crime—witness the computer dating bureaus which lure their marks with false promises of the computer and its accompanying mystique.

Our experience at the Department of Justice and the findings of the GAO report indicate that the largest incidence of computer crime today falls into this broad second category.

In the third category, the computer acts as an accomplice.

Highly trained, highly skilled "computerniks" massage and manipulate the computer to the point that it becomes an unwilling accomplice in the theft of computer time, programs, sensitive information, cash and other assets.

These schemes range from the simple to the highly complex. On one hand, a bank programer may insert a single "patch" in the bank computer program which will cause the system to ignore his overdrafts. Other more sophisticated "computerniks" engage in complex cryptography to break the computer's access code, manipulate the internal systems in order to perpetrate the crime, and then program the computer to destroy all traces of the unauthorized intrusion.

There may be a great temptation on the part of some computer users and law enforcement officials to dismiss this brand of computer crime as science fiction. To do so would be a serious mistake. It is a reality today and in all probability will constitute the majority of computer crime in the future.

Consider for an example a five-digit access code. To break that code by the trial and error method would require 100,000 combinations—statistics which would deter the average person from such an approach. But for the intruder with a computer accomplice the password becomes meaningless. In one instance, the user of a time-sharing system with general access to the computer wanted to get access to information locked in a higher security level beyond his authorization; he programed the victim's own computer to try all possible combinations of the higher level access code. Several seconds and several thousand combinations later, the computer successfully "picked the lock."

The message for law enforcement is clear—one must not underestimate the computer-assisted criminal. There are over 1 million computer programers in the United States today. And those individuals who build and design our computer systems will always have the keys to unlock them.

The prosecution of computer crime is hindered by a number of factors. Computer crime is a low visibility proposition. There are no smoking pistols—no blood-stained victims; often the crime is detected by sheer accident. Recently, a squib buried in the business section of a Washington newspaper caught my attention. The gist of the article was that a major industrial firm had relocated its toy division. In the relocation process, it suspended its computer operation and conducted a physical inventory, only to discover $1.5 million in missing inventory. In all probability if it had not been for the fortuitous relocation, the deficit would have widened.

To further illustrate this important point, several years ago the New York City police raided a gambling operation and recovered a list of bookie's customers. The book indicated that one customer bet upwards of $30,000 per week. A background check revealed that he was an $11,000 per year programer at a New York City bank. By manipulating customer accounts, he had embezzled more than $2.5 million over a period of years. While this specific investigation represents coordinated police work at its best, it is not particularly comforting from a broader perspective.

To compound the problem, users are often reluctant to report computer abuse because of the embarrassment that such disclosure might bring. The major accounting firms increasingly receive audit requests from corporate officials who suspect computer abuse. In a recent case brought to my attention, an outside audit commissioned by bank officials confirmed that a computer programer had manipulated the bank's data system and embezzled $250,000. However, fundamental errors in the design and implementation of the bank's computer system had resulted in an additional $10 million in losses through negligent overpayments, miscalculated interest, and uncollected charges. The bank directors were in no mood for the publicity of a public prosecution. They took the position that the embezzler had done them a great service by exposing the deficiencies of their system and saving them from an avalanche of shareholder suits and possibly bankruptcy.

One might ask how a sophisticated banker or other computer users could find himself in the predicament illustrated in my last example? Computer users are curiously ambivalent about security. Consider the businessman who would never leave his checkbook lying on top of his desk—who requires a double signature on each corporate check—who would never discharge a sensitive employee without changing the lock on the door and the combination of the office safe—and who would be aghast if his banker informed him that as an economy measure the bank was no longer returning canceled checks. This same businessman will purchase a multimillion dollar computer system from an energetic salesman without an audit as basic as a canceled check—will place a computer terminal on top of the desk unattended—will use one programer to design his entire computer system—and will discharge his programer without making the most rudimentary changes in his computer's security system.

In addition to the problem of undetected and unreported crime, the computer-related cases that have been prosecuted have often ended in a guilty plea without a reported opinion; many that have gone to trial are presently on appeal. As a result, there is presently more computer law in the newspapers than in the case books. Because of this timelag, we simply are not in a position to accurately gage whether traditional laws are adequate to deal with the problem.

At the Federal level, we have been successful in prosecuting under the wire fraud statute, as in a recent Maryland case involving the owner of a computer firm who stole a valuable confidential program by tapping into his former employer's computer center by long-distance telephone. Basically, the wire fraud statute imposes criminal sanctions for engaging in a "scheme to defraud" by use of interstate wire signals: telephone, telegraph, and other forms of wire communication between States. The broad concept of a "scheme to defraud" conveniently fits most computer tampering and a significant number of cases do involve wire communication across State lines.

The interstate requirement does, however, produce an arbitrary result in certain situations. For example, had the defendant in the Maryland case placed the crucial telephone call to the Rockville, Md., computer from his home in Maryland instead of his office in suburban Virginia, there would have been no Federal jurisdiction. If the Federal Government is to invest considerable resources in developing a capacity to deal with sophisticated computer crime, it is questionable whether Federal jurisdiction should turn on such an arbitrary distinction. Assuming wire fraud jurisdiction were to be expanded to reach any use of the facilities of wire communication, regardless of whether the actual signal travels between States, we would close an unnecessary loophole in Federal criminal jurisdiction—not only for computer crime but conceivably other fraudulent schemes as well.

In certain narrow factual situations, other Federal statutes may be applicable to computer crime. If a Federal computer facility is victimized, the fraud against the Government or theft of Government property statutes may be available: if the computer tampering results in the issuance of fraudulent checks by mail, the mail fraud statute could be used; if the crime results in the unauthorized movement of merchandise or other property across State lines, the interstate transportation of stolen property statute ("ITSP") may be applicable. In the computer context—particularly if the item stolen is information, programs, or other intangibles and the victim is not actually denied physical access to the stolen property—a prosecution based on the latter provision may be hindered by the traditional definition of "property" and "theft" and the concept of a "taking." For example, in the Maryland prosecution mentioned earlier, the Court dismissed the "ITSP" count on the theory that the movement of the magnetic impulses from the victim's computer in Maryland to the defendant's computer in Virginia, did not satisfy the interstate transportation requirement of the offense. State prosecutors without the benefit of an expansive wire fraud statute will more frequently encounter these definitional problems, as discussed in greater detail later in my remarks. At the Federal level, consideration should be given to appropriate amendments of the criminal code to clarify these uncertainties.

The new Federal Rules of Evidence, effective July 1976, will assist our prosecutors by bringing computer records squarely within the business records exception to the hearsay rule: Rule 1001(1) defines writing and recording to include magnetic impulses, mechanical, or electronic recording and all other forms of data compilation; more importantly, rule 1001(3) provides that if data is stored in a computer or similar device, any printout or other output, readable by sight and shown to reflect the data accurately, is to be considered an original. This last provision will be extremely helpful not only from a logistical standpoint but also due to the fact that intermediate computations within a computer system are often unretrievable.

Questions remain, however. The prosecution still has the burden of establishing the authenticity of the computer records by introducing evidence describing the particular data processing system and demonstrating that the system produces an accurate result. This will require the most careful witness preparation to insure that the Government expert communicates in a language that the court can understand. Such authentication may be difficult for a computer system with a track record of malfunction or without those error detection devices commonly used in the industry. Furthermore, the Federal rules leave unresolved the possibility that courts in certain situations may still require the introduction of the original input document, for example, sales slips, invoices, purchase orders, et cetera.

For State and local prosecutors without a counterpart of the wire fraud statute or the certainty of the Federal Rules of Evidence, the path to conviction may be even more torturous. A California State court, in a trade secret prosecution involving the theft of sensitivity programs by remote access closely analogous to the Maryland case discussed earlier, held that the electronic impulses which the defendant extracted from the victim's computer were not an article representing a trade secret; instead, the court held that the paper printout of these impulses constituted a copy of a trade secret and this copying was actionable under California law. The court's distinction was unfortunate. Under the court's reasoning, had the defendant fed the stolen program directly into his computer or had he displayed the program on a visual screen instead of printing it out on paper, no crime would have been committed.

In other prosecutions based on commonlaw theft concepts, we encounter additional problems: The distinction between theft and grand theft is muddied where the stolen property is information whose monetary value may be difficult for the court to determine. In the large time-sharing systems which are the trend today, thousands of individual users commingle their data in central files with loose security restrictions, and the concept of trade secrets and the even more basic distinction between public and private property may be lost to a jury. The penalties which a court may impose on the computer criminal may not serve as a sufficient deterrent. Computer crime lacks the traditional indexes that give rise to stiffer sentences: There is no physical contact, no use of firearms, no breaking and entering. For example, under typical State trade secret laws, it is a felony to break and enter to obtain a trade secret, but only a misdemeanor to gain unauthorized access to trade secret information. In both the California case and the Maryland case the defendant broke and entered the computer systems but it is extremely doubtful that a court would consider this electronic intrusion as commonlaw breaking and entering.

To attempt to resolve some of these questions, the Justice Department has begun a comprehensive evaluation of the computer related cases, including those cases outlined in the GAO report. We are not limiting our attention to reported opinions. In many instances such as the *Equity Funding* case which ended in guilty pleas, key legal issues are addressed in plea bargaining negotiations and pretrial hearings and motions which are never reported. By interviewing those investigators and prosecutors who have had direct involvement with the case, we hope to determine the proper role of the Department of Justice in the computer crime area—to assess the possible need for new legislation or investigative techniques.

Second, we believe it is important to give as many of our investigators and attorneys as possible a basic familiarity with computer operations, and at the same time, develop a mechanism to provide us with the specific and highly professional expertise that we will need periodically for major computer fraud cases.

In July [of 1976] the U.S. attorney's office in San Diego, in cooperation with the University of California, sponsored a week-long seminar in computer fraud for State, Federal, and local prosecutors in the western region. Each attorney was given an introduction to computer science; each was able to write his own programs and develop a working familiarity with the computer—at least on a rudimentary level. The attorneys were given simulated case studies. Working directly with computer center personnel, they were taught to identify the hypothetical fraud and to obtain the evidence from the computer necessary to prosecute their case. Such training will be indispensable in the future.

The prosecution of white-collar crime invariably involves a "paper chase." Evidence is buried in the books and records of the suspect: His checks, deposit slips, receipts, accounts, and ledgers. In the computer context, this paper is replaced by electronic impulses buried in the memory of the computer. To capture this evidence intact becomes a new challenge for the prosecutor; a challenge which is accentuated by the microsecond speed with which computer records can be altered or destroyed without a visible trace.

Prosecutors must recognize these distinctions and adapt their investigations accordingly. In the past we have relied extensively on the grand jury subpena as an investigative aid. However, one disadvantage of the grand jury subpena is that it relies on the target to bring the incriminating evidence into court. In a surprising number of cases, the suspect will unwittingly incriminate himself. This is usually a result of fact that the investigation has not focused; the suspect's files are voluminous and he simply cannot efficiently segregate the incriminating from the innocuous. Also, there are generally so many photocopies in circulation that an attempt to destroy one set of documents would be counter-productive. In the future, centralized data banks will frequently eliminate the need for Xerox copies. A well indexed data base will give the target an opportunity to identify and selectively alter incriminating information.

Thus, it may be increasingly important to seize the suspect's books and records before they can be altered or destroyed; the investigator may be forced to rely increasingly on the search warrant procedure. The prosecutor must have sufficient knowledge of the computer system to draft a warrant that is broad enough to reach the evidence but sufficiently narrow to withstand challenge. Nor would it be productive for the investigator to arrive on the scene with a valid search warrant if he cannot get the data out of the machine or to put a guard at the door if the computer operator inside can instantaneously destroy evidence with the push of a button. These new circumstances must be carefully understood and explained to the magistrate at the time a search warrant is requested. Extraordinary procedures may be warranted; the Government may be obliged to seek a court appointed receiver to assume operation of the data system to insure the evidence is not destroyed and to enable the Government to recover data in a meaningful format.

Once the prosecutor has obtained his evidence, he must be aware of still other technological peculiarities. Information stored in a computer memory is extremely volatile. Magnetic tapes and discs must be stored at carefully controlled temperatures and atmospheric conditions. The prosecutor who locks a computer tape in a file cabinet of a Government building with no air-conditioning on the weekends, may inadvertently destroy his evidence or at least expose it to challenge by the defendant's more computer-wise attorney.

The most compelling reason for exposing our attorneys and investigators to basic computer operation is to encourage the use of the computer as a positive law enforcement tool. In the late 1960's the FBI developed a computer-assisted technique to classify fingerprints which led to identification of James Earl Ray as Dr. King's assassin. The FBI is now employing a similar technique to sift through thousands of latent fingerprints from unsolved crimes in an attempt to match them with fingerprints on file in the Bureau records—a task which would have been humanly impossible without computer assistance.

Recently, the U.S. attorney in Seattle used the computer to successfully prosecute the owner of an independent telephone company who had devised an intricate scheme to defraud A.T. & T. on the calculation and distribution of long-line telephone revenues. The prosecutor used the local public utility commission's computer to reconstruct the crime relying on a theory similar to the net-worth theory of tax fraud. The prosecutor, working closely with his computer experts, painstakingly explained this theory to the court, and obtained a conviction that was confirmed on appeal. Constraints of man-hours and resources might have ruled out this prosecution had it not been for imaginative use of the computer. At the present time, the Justice Department is also using the computer to collect and categorize voluminous records at the heart of a major land fraud investigation. As the Senate demonstrated by its effective use of the computer throughout the Watergate hearings, the ability to instantaneously access information in a meaningful way can greatly assist the prosecution's case. In short, the same computer that facilitates the crimes we have discussed can be a powerful tool in the hands of law enforcement officers who know how to use it effectively.

Each technological advance—whether in weaponry, transportation, or communications—breeds a new genre of crime. Each technological advance demands a new response from law enforcement. [We] should focus the attention of all law enforcement agencies on the power of the computer—both as a tool of crime and a tool of law enforcement. At the same time it is our hope that businessmen and other users [will be alert] to the computer's inherent vulnerability. The computer user is the first line of defense; he must take steps to protect himself.

THE JERVIS FINNEY STATEMENT

In connection with his request of information from Richard L. Thornburgh, the Assistant Attorney General in the Criminal Division, Senator Ribicoff also wished to obtain information from a U.S. attorney who had actually been in charge of the prosecution of a computer crime. Accordingly, Senator Ribicoff asked Jervis S. Finney, the U.S. attorney for the District of Maryland, to provide the committee with a statement concerning a computer abuse case which fell within the jurisdiction of Mr. Finney's office. On January 5, 1977, Finney submitted the following letter and statement to the committee:

JANUARY 5, 1977.

Hon. ABRAHAM RIBICOFF,
Chairman, Committee on Government Operations,
U.S. Senate, Washington, D.C.

DEAR SENATOR RIBICOFF: In response to your request, I am enclosing my statement on behalf of the U.S. attorney's office for the District of Maryland concerning the subject of the experiences encountered in the prosecution of computer-related crime. The issues addressed in this statement concern two computer-related prosecutions recently concluded by this office. We have not commented generally on all aspects about the recent developments in this area since the memorandum submitted by Richard L. Thornburgh, Assistant Attorney General of the U.S. Department of Justice and the report of the General Accounting Office have adequately reviewed these matters.

Yours very truly,

JERVIS S. FINNEY,
U.S. Attorney.

With the advent of the computer age, it was inevitable that the age of computer-related criminal activity would follow. Perhaps no where is this better witnessed than in this federal judicial district where, during the past year, two computer-related prosecutions have been successfully concluded.

I.

The first, and the more noteworthy, is *United States of America* v. *Bertram Seidlitz*, in which the computer was used as an accomplice. Briefly, the facts in that case were that Seidlitz had been gaining unauthorized access to computers operated by Optimum Systems, Inc., Rockville, Md., a firm which provides computer services to the Federal Energy Administration. Optimum Systems, Inc. (OSI), had previously developed a software package known as "Wylbur" which had been used to obtain contracts with various Government agencies including the Federal Energy Administration. Although the Wylbur software package was one of the most sophisticated which had been developed, it was still necessary to make certain refinements in it to meet the specifications of the Federal Energy Administration contract.

Seidlitz, while employed at OSI, had been assigned to the OSI–FEA project. In that capacity he obtained the necessary access codes to the computer system which he retained after he terminated his employment. Thereafter, armed with this information, a remote computer terminal, and an ordinary telephone, Seidlitz simply dialed the computer's telephone number at OSI in Rockville and requested various portions of the Wylbur software package, through the use of certain initials, account numbers and access codes. This information would then be transmitted, by electronic impulse, over the telephone lines to Seidlitz's computer terminal which he maintained at his computer business in Alexandria, Virginia. The electronic impulses would be transformed into a standard computer printout. Evidence produced indicated that Seidlitz accessed the OSI computer on at least 40 different occasions spanning approximately 4 months. Further, it appeared that Seidlitz had been using the computer to establish his own data sets.

As often occurs in computer-related crimes, detection occurred by accident. Once the unauthorized access was discovered, agents of the Federal Bureau of Investigation, in conjunction with employees from the telephone company, were able to trace the telephone calls from the computer to both Seidlitz's office in Virginia and his residence in Maryland. Federal search warrants were issued for both addresses and computer printouts were seized at his office while the portable terminal was seized at his residence. Subsequently, Seidlitz was indicted on two counts of wire fraud (title 18, U.S.C., section 1343) and one count of interstate transportation of stolen property (title 18, U.S.C., section 2314).

It is readily apparent from this cursory description of the evidence that numerous difficulties are encountered not only in the prosecution of a computer related crime, but also in the investigation. For example, even after the original detection of the unauthorized user has been made, law enforcement officials are hampered by the reluctance of the private industry sector to supply agents with information. If telephone trace is instituted, at the victim company's request, telephone officials are hesitant to supply any information to investigators without prior judicial approval. If the identity of the suspect has been established, it is also incumbent to establish, with precision, what material is being retrieved from the computer. Unless the victim company has certain specialized equipment available, this may pose an extreme burden which can seriously hamper any attempt to obtain a search warrant.

Once these obstacles are surmounted, and a search warrant issued, investigators are confronted with yet another impediment: How to identify the stolen material. In the Seidlitz case, investigators were fortunate since the computer printouts had not been destroyed or transformed to another medium. But, for instance, what would have occurred if Mr. Seidlitz had transferred the information on the computer printout onto magnetic tapes and stored the tapes along with the thousands of other magnetic computer tapes in his data processing center? Would investigators have been justified in seizing all of the tapes or would they have been required to determine, at that point, which of the tapes contained the information sought by running the tapes on the computers? Moreover, all of the (in our view, unjustified) advantages enjoyed by white collar criminals are available to the perpetrators of computer fraud.

For Federal prosecutors, the obstructions to be hurdled are equally enormous. Presently, there exists no Federal legislation which specifically is intended for computer-related crimes. Thus, the wire fraud statute is useful if it can be proven that an interstate communication was made; on the other hand, if Seidlitz had used his residence as his base of operations to obtain the computer program, then the wire fraud statute would have been useless. Nevertheless, it is noteworthy that in the Seidlitz prosecution the telephone traces which were made to Seidlitz's residence in Maryland were admitted in evidence by the court as a similar act to establish the identity of the unauthorized user; other courts might not have displayed such wisdom.

Another prohibitive element of the wire fraud statute is the establishment that such a scheme to defraud was for the purpose of obtaining "money or property." There has been some discussion in the legal community whether computer programs and software packages are "property" or are merely concepts. In *Seidlitz*, the court ruled that there was a factual predicate for finding that the "Wylbur" program developed at OSI and used to obtain the FEA contract was a "trade secret" and was, thus, enveloped within the term "property."

In support of its determination the court relied upon *Hancock* v. *Decker*, 379 F. 2d 552 (5th Cir. 1967) which is one of the few reported cases involving computer fraud. The court specifically held, in that case, that the programs contained on printouts were property and the term "property" was not limited solely to the actual paper upon which the various data sets and other computer information was written.

In addition to the two counts of mail fraud, Seidlitz was charged with violation of title 18, U.S.C., section 2314, interstate transportation of stolen property. In granting the motion for judgment of acquittal as to this count only, the court stated that there was no asportation of property since the program remained in the victim computers in Maryland. Unlike those cases in which a photocopy of the information is made and then transported interstate the only "thing" which was transported in interstate commerce were electronic impulses crossing through telephone lines. See, for example, *United States* v. *Bottone*, 365 F.2d 389 (2d Cir. 1966) for a discussion regarding photocopies information. Thus, the court did not believe that there was sufficient asportation of any "property" as embodied within the statute.

In certain circumstances, a suspect could be charged under 18 U.S.C. section 641, theft of government property. In Seidlitz, the statute was inapplicable since it was clear that the programs were the property of Optimum Systems, Inc. However, an argument might have been made, under the facts of this particular case, that at least certain data sets were developed specifically by OSI for the FEA in accordance with the contract. Under such theory, it could have been argued that Seidlitz stole information which had been made under contract for the United States in violation of the second provision of section 641 of title 18, U.S.C., which provides, in pertinent part:

> "Whoever embezzles, steals, purloins or knowingly converts to his use or the use of another . . . *any property made or being made under contract for the United States* or any department or agency thereof. . . ."

Thus situations may arise where although the programs are not actually government property, they have been made, or at least modified, for use by a federal agency in acordance with a specific contract. Absent any other applicable statute, this statute should be considered.

II.

The second prosecution in this district concerned the more usual type of computer-related crime in which the computer acted merely as the environment for the crime. In this case, no specialized knowledge of data processing or computer programing was necessary and the criminal was not required to be a computer scientist. In *United States of America* v. *Amy Everston Jones*, evidence produced showed that the defendant's brother, Michael Everston, was employed at Inglis, Ltd., a Canadian appliance firm affiliated with Whirlpool Corporation. In this capacity, Everston instructed a keypunch operator to open a new account in the name of his sister and assigned a new vendor code number to her. Then, on certain occasions, Everston would substitute the Whirlpool vendor code number with his sister's code number on the accounts payable distribution slip without disturbing the other information on the slips including the amount due.

Thereafter, he would give such information to the keypunch operator who would place the information on data processing cards. This information was programed into the computer where it remained for approximately 2 weeks. In the interim, Mr. Everston would retrieve the accounts payable distribution slips from the keypunch operator, and return the correct vendor code to them to avoid detection. Then, the corporation would instruct the computer, in accordance with the information in its program, to create a check run to pay the accounts payable. The computer would issue the checks as programed complete with facsimile signatures of the corporate officers. Obviously, checks would be issued to Everston's sister in Maryland instead of to the Whirlpool Corp. The total amount of checks deposited in Maryland was in excess of $132,000.

Again, the scheme was detected not by sophisticated auditing procedures or other safeguards, but by chance. Miss Jones was charged in Maryland with interstate transportations of securities in excess of $5,000 which were stolen, converted and taken by fraud, knowing the same to have been so taken in violation of 18 U.S.C., section 2314. The defendant was also charged with receiving such securities which had travelled in interstate commerce in violation of 18 U.S.C., section 2315.

In dismissing the indictment the court held that the checks issued by the computer were forgeries since the computer, itself, was acting as the agent of Everston rather than the agent of the corporation. In its reasoning the court concluded that if the checks were forgeries then the indictment would be required to be dismissed since the exclusionary provisions of each section provides that the sections should not apply to falsely made or forged securities issued by banks or corporations of a foreign country. Thus, since the checks were issued by a Canadian corporation and were, under the court's reasoning, forgeries, then the indictment was invalid.

The matter was appealed to the U.S. Court of Appeals for the Fourth Circuit where it is presently pending. It is the government's contention that the computer, as an inanimate object, was owned by the corporation and was acting on the corporation's behalf and was not acting as the agent for Everston. In support of such contention the government has argued that the signatures which were placed on the checks by the computer were genuine but were based upon fraudulent information supplied by Everston.

It is noteworthy that if the district court's holding is correct that such checks issued by computers based upon fraudulent information were forgeries, appropriate criminal sanctions will be lacking in many instances where securities are issued by large international corporations doing business in foreign countries. The only other available Federal statute would possibly be a mail fraud statute (title 18, U.S.C., section 1341) but such statute, similar to the wire fraud statute, requires proof that documents were placed in United States mails in furtherance of the scheme to defraud. Thus, there may be instances where computer-related criminal activity has no criminal sanction.

The report by the General Accounting Office confirms that computer-related criminal activity will be an ever increasing problem in the future. Traditional investigative techniques and traditional criminal sanctions may well be antiquated. Legislation addressing the specific problems of computer abuse will be mandated as the criminal mind uses the computer in ever increasing ways to fulfill his schemes. It is respectfully submitted, therefore, that Congress consider legislation which would prohibit unauthorized use into computers owned by, operated for, under contract with, on behalf of, or in conjunction with the U.S. Government. Such legislation would alleviate difficult issues for the court such as whether a software program is property, whether there has been asportation of any property and whether such property traveled interstate. Although such legislation would have the limitation that only computers associate, in some form, with governmental use would be covered, it is respectfully suggested that much of the computer-related criminal activity has involved governmental agencies or computers acting on behalf of the agencies.

Further, it has been suggested that the wire fraud jurisdiction be expanded to reach *any* use of the facilities of the wire communication, regardless of whether the actual signal travels interstate. Such legislation, if constitutional, would be of an enormous benefit to prosecutors since it would eliminate the burdensome element of proving the exact source of the telephonic communication. It would also eliminate, as shown in the *Seidlitz* case, difficulties which arise when dealing with third party such as telephone companies who are unwilling to supply law enforcement agencies with information until a time consuming judicial document is obtained. Lastly, it is respectfully suggested that with the voluminous number of checks and other securities issued by computers in both the public and private sector, definitional guidelines be established which would clarify whether such securities are forgeries if issued on the bases of improper or fraudulent data. In doing so, the difficulties experienced in the *Amy Jones* case could be eliminated.

Certainly, imaginative legislation must be enacted to deal with futuristic crimes which are becoming more commonplace in modern society.

THE FEDERAL BUREAU OF INVESTIGATION

Senator Ribicoff asked Clarence M. Kelley, Director of the Federal Bureau of Investigation, to comment on computer crime and computer technology. On November 16, 1976, FBI Director Kelley submitted this statement to the committee:

> The FBI is involved in today's fast-moving, technical environment of the computer by using computers to investigate crime and investigating crimes which involve computers. The FBI also uses computers to alleviate part of the Bureau's administrative burden to allow maximum attention to our investigative mission. In these capacities, the FBI maintains an awareness of computer security to protect its own systems and to investigate crimes involving other computer systems.
>
> As the FBI places more emphasis on white collar crime, our special agents often are confronted with increasingly complicated cases. Since investigation of major frauds requires the special agent to collect and organize massive volumes of evidence and other investigative information, the FBI is now using computers to do this in a more accurate and expeditious manner. On several occasions special agents have seized evidence in computerized form and FBI computers were used to organize and sort the information in preparation for trial.
>
> Computer technology is used as an investigative management tool in major cases in which several hundred special agents conduct thousands of interviews. A major case information system has been developed which produces an automated index to the manual investigative files of such major cases. This system has been used in the Watergate case, the Hearst kidnapping case, the killing of two special agents on the Pine Ridge Indian Reservation, the bombing of the LaGuardia International Airport, and others.
>
> Although FBI investigative files are not automated and the FBI has no plans to automate them, we have been involved in automating the existing manual functions which provide access to our files, maintain document accountability, and maintain file location. Eventually we will have a fully automated index to the investigative files. At the same time we are upgrading our existing communications facilities by implementing a computer-controlled network.
>
> Virtually all FBI functions, both investigative and administrative are supported by computers. The FBI is totally committed to, and dependent on, the continued development and implementation of supporting automated information systems. The FBI's computer staff is able to respond immediately to almost any investigative information processing need.
>
> The National Crime Information Center (NCIC) is a nationwide on-line information system which contains over 6 million records of stolen property, wanted and missing persons, and criminal histories. Designed to provide information to Federal, State, and local criminal justice personnel on a timely basis, NCIC is managed and financed by the FBI;

however, the entire criminal justice community participates in its operation and actually uses it on a nonreimbursable basis. The FBI maintains system security to the State level and each State manages system security within its State. It should be noted that information regarding stolen property and wanted and missing persons is public record information; however, the presence of criminal history information in NCIC necessitates appropriate protection as required by the Privacy Act of 1974.

The FBI Identification Division has been the national repository for fingerprint records since 1924. Arrest fingerprint cards form the basis of a centralized criminal history record information system. To cope with the tremendous volume of fingerprint cards, disposition sheets, and inquiries received each day (approximately 22,000), the FBI began using computers in the Identification Division work in 1974 by automating the arrest records of all first-offender criminals. In addition, this effort toward the automation of the Identification Division includes the installation of automatic fingerprint-reading equipment. The information collected, maintained, and disseminated by the Identification Division is personal information and is afforded appropriate privacy protection.

In view of the FBI's extensive experience in using the computer as an investigative tool, a 44-hour course entitled "Introduction to Electronic Data Processing for Law Enforcement," has been added to the curriculum of the FBI National Academy, which is attended by officers from numerous law enforcement agencies. This course, accredited by the University of Virginia, is designed to present a general introduction to the concepts and basic features of computers. Emphasis is directed to the proper use of data processing and to the role of the computer in law enforcement; that is, as a law enforcement tool, and as an aid in law enforcement management, administration, operations analysis, and operations planning.

In addition to using computer technology, the FBI investigates crimes in which computers are involved. When valuable computer hardware is stolen or destroyed, law enforcement officers investigate the crime just as they do when any other valuable piece of property is stolen or destroyed. The identical investigative approach may not suffice in solving a computer crime which involves intangible computing resources such as computer programs (called software), computer time, and data. Computer crimes can sometimes be committed via a telephone network by using an appropriate remote terminal which can be purchased for a few hundred dollars.

The FBI recently investigated a computer crime which involved the illegal penetration of an on-line Government computer system through the use of a remote terminal device. The agency officials believed that the system was penetrated by computer experts. The initial phase of the investigation entailed obtaining a complete description of the agency's organizational structure and the system security plan. The agency, in accordance with Office of Management and Budget Circular A–76, had obtained computer facility management services from a private computer company. The agency's officials believed that such an arrangement was an excellent means of operating a Government computer system because the employees of the private company could be hired and fired at will.

Special agents investigating the case determined there had recently been some employee changes made on this Government account and immediately recognized that the most likely security vulnerability of the computer system was the "disgruntled employee." Upon request the officials of the private company identified six ex-employees as possible suspects. After obtaining a court order the special agents traced telephone calls which were made into the computer system and discovered the calls were being made from the business telephone of one of the six ex-employees. As the investigation continued, the special agents learned this particular individual had been one of the key programers on the Government account.

The ex-employee was charged with fraud by wire. At his trial he claimed he was only demonstrating system security vulnerabilities and would later seek a contract with the Government agency as a security expert. Since his efforts had been concentrated toward copying a single computer program and he did not attempt to obtain other classified or proprietary data, it was obvious that he was not simply testing the system's security. He intended either to use or sell all or portions of the copied computer program at a profit. He was convicted and was sentenced to 3 months in jail and 3 years of probation. Like other publicized computer criminals, he is now advertising himself as a security expert.

Computer systems which contain classified national security information are possible foreign espionage and sabotage targets, and intelligence activities directed against these systems fall within the FBI's investigative responsibilities. Government and private systems which do not contain classified information also should be recognized as targets for theft of data. Government and private industry computer systems which contain proprietary information and industrial secrets are industrial espionage targets. Industrial espionage activity which involves theft of data or information could be investigated and prosecuted by the Federal Government as "Interstate Transportation of Stolen Property" or patent or copyright violations.

Another complex computer crime which involves theft of an intangible asset is the unauthorized use of a computer. Computers can be illegally used by either individuals with authorized access to the computer site or by unauthorized individuals through communication lines and remote terminals. An employee misusing a Government-owned computer could be charged with fraud against the Government. The FBI has investigated a few cases involving misuse of Government computers by employees; however, to date none have been prosecuted.

A type of computer crime which has received much publicity recently involves the fraudulent act of an employee who attempts to enrich himself by manipulating the data in a computer system which maintains banking records. This type of crime does not necessarily have to be committed by a computer programer or operator. In fact, it is usually committed by clerical personnel who discover a vulnerability in the way the computer handles banking data. Even though computer systems which maintain banking records have built in audit trails, crimes directed against these systems seldom, if ever, are discovered by system audits. The crime is typically discovered by accident, as happened, for example, when police conducting a surveillance of an illegal gambling establishment observed a bank clerk enter the establishment on several occasions. It was subsequently discovered that he was taking advantage of a vulnerability in a computerized bank system to embezzle funds from the bank.

On many occasions the employer has discovered all aspects of the crime and the special agent investigating the crime simply interviews the embezzler and documents the incident for presentation to the U.S. attorney. As the computer criminal becomes more sophisticated, investigations of these crimes will become more complicated. The special agent assigned to these cases must have a basic understanding of computer technology. He will seek the cooperation of the internal auditor of the victim bank or company in order to identify the embezzler.

Computer systems which issue checks or order supplies are often designed as decisionmaking systems. It may be possible for a key employee, either clerical of technical, to issue funds to many unauthorized individuals who have several false identities and defraud the Government of a substantial amount of money in a short period of time. When computers are used to manage logistic or supply information systems, the computer data base is actually an ownership file. An individual with access to the system can illegally obtain supplies. This computer crime can be committed either by an employee or by an outsider penetrating the system through communications lines and a remote terminal. Proper audit trails on decisionmaking systems should be established to prevent computer crime and assist the investigator if a crime is attempted. Whenever possible check-issuing systems or logistic systems should be designed to require the actions of two or more employees so that one, by himself, cannot commit a fraud. The FBI payroll system is designed in such a manner and is not by definition a decisionmaking system.

In August 1974, $17,000 worth of aircraft radios disappeared at a military base. The investigation revealed that approximately $90,000 in additional property had been diverted from the custody of the Government. These thefts were being concealed through the use of fraudulent procedures in operating the computer system which processed equipment orders. The criminals created fictitious requisition forms by computer. The Government property was diverted to innocent civilian contractors who were subsequently contacted by the criminals, or their representatives, and advised that the shipment was misdirected. The criminals took possession of the property and then erased the identification records of the property from the computer system to insure that the periodic computer audit reports would not reveal illegal activity. Investigation revealed the criminals received in excess of $400,000 from the sale of the stolen property. It was estimated that this computer crime resulted in a $2 million loss of property. The investigation of this case was so complicated that a special agent, who is assigned management duties on our computer staff, was assigned to manage the case and provide technical guidance. Three of the criminals received 6 years in jail, one criminal received 4 years and one criminal received 3 years probation. A total of $78,000 in fines was imposed.

Finally, the problem of the computer equivalent of the phone "freak" should be mentioned. Phone "freaks" have raised havoc using "blue boxes," that is, special electronic devices built to avoid paying for phone calls. The phone "freak" usually is not motivated by potential monetary gain. He sees the telephone system as a challenge and tries to defeat it. This same attitude now is spreading into the computer field. The combination phone "freak"-computer "freak" attacks on-line dial-up computer systems via regular telephone lines with an inexpensive remote terminal. He may completely sabotage the system instead of trying to obtain any monetary benefits.

Realizing that computer crime would be a crime of the future, the FBI began a program to train special agents in computer technology. Since January 1974, the FBI has trained over 500 special agent accountants in the fundamentals of data processing. Each of these agents has been given 2 weeks of instruction on basic computer concepts, including the conversion and storage of data, and the processing and retrieval of data. A discussion of various computer-related crimes and computer frauds was part of the training curriculum. Recently the FBI began giving similar instruction to agents who do not have degrees in accounting, but are working white collar crime cases. Over 200 of these agents eventually will be trained in the fundamentals of computers and the investigative techniques of solving computer-related crimes. A new, specialized course of 4 weeks' duration is being given to special agents who have expressed an interest in pursuing an in-depth study of investigative techniques of computer-related crimes, with emphasis on those crimes most frequently perpetrated in a banking environment. This education program will insure that the FBI will have special agents throughout the country who are qualified to conduct thorough investigations of computer crimes. We also have 13 special agents assigned to our computer staff at FBI headquarters in Washington, D.C. Each of these special agents has several years of technical experience in the application of computers and is available for temporary assignment to the field offices to assist in the more complicated cases.

Because most computer crimes are the investigative responsibility of State and local law enforcement and some computer crimes are the investigative responsibility of other Federal agencies, the FBI is providing computer crime and white-collar crime training to Federal, State, and local investigative personnel. In September 1976, investigators from the Department of Health, Education, and Welfare attended a 2-week FBI course on computer technology and white-collar crime. Also, the introductory computer course which is now part of the FBI National Academy curriculum equips the local law enforcement attendees with the necessary skills to investigate all but the most complex computer crimes which may fall within their jurisdiction.

As previously indicated, the FBI maintains an awareness of computer security to protect its own system and to investigate computer crimes properly. "Computer security" can be defined as the mechanisms and/or procedures designed and implemented to protect computing resources from illegal action. Since computer security is a management problem as well as a technical problem, management must protect all computing resources, including hardware, software, physical sites, employees, documents, and data. Because security in total is only as strong as the weakest link in the "security chain," it must be applied in a balanced method. Virtually all computer security experts advocate use of a total system risk analysis methodology to evaluate and implement security. It is neither functionally nor economically feasible to select generalized security features and apply them equally to all automated information systems. Only reasonable and appropriate security features should be applied to each system and computer security cost must be included as a portion of the total system cost when conducting cost analyses. It must be recognized that, just as in the case of all security matters, perfect computer security is not attainable; however, adequate security safeguards can be developed for each system to allow the use of computers with an acceptable level of risk.

Even if the computer security plan is very sophisticated, a good audit, test, and certification program must be implemented by computer users. Audit trails must be maintained by the system and must be examined objectively on a regular basis by independent personnel. Auditing must never be conducted by bypassing the computer. The computer itself must be audited. Consideration should be given to testing security by having independent personnel attempt to penetrate the system.

The FBI is concerned with the protection of its own automated information systems. Some of our computer systems do contain classified information, but the majority contain information requiring appropriate security safeguards as set forth in the National Bureau of Standards "Guidelines for Implementation of the Privacy Act of 1974." Computer security policy for the protection of classified national security information, which is maintained and processed by automated systems or networks, is developed by a Computer Security Subcommittee, on which the FBI maintains active membership, under the direction of the Director of Central Intelligence. In addition to the computer security guidelines and policies which must be followed by all Government agencies, the FBI has its own policy which goes beyond the minimum required.

Use of computers by the Government is regulated by Office of Management and Budget (OMB) circular A-76 and the Brooks bill (Public Law 89-306). Those concerned with computer security in Government systems should be aware that OMB A-76, which requires Government agencies to obtain all services, including computing services, from the private sector whenever possible, does not permit agencies to exempt systems from the private sector because of stringent security requirements. In the computer area, just as in any other area, the level of security can only be as high as the trustworthiness of the personnel who design and operate the system. Given the transitory nature of personnel in the private computer sector and the fact that a lot of work is done on short-term contracts, it is difficult to insure the reliability of all vendor personnel. That is not the case with career Government employees. The Brooks bill, which requires competitive procurement of computer services, does not present the Government with major special security problems since it is usually possible to structure functional statements of the computer service to be procured in terms that are unclassified.

This paper has endeavored to set forth information regarding: (1) the FBI's use of computers, (2) the many facets of computer crime, (3) FBI computer training programs, and (4) computer security. The FBI was one of the first Federal Government agencies to use computers, and we have grown slowly and deliberately into the computer age. We have many applications which directly support our operational mission, and our applications are sufficiently secure. Our training program and the assignment of special agents to our computer staff have prepared the FBI to cope successfully with the computer crimes of today and the future.

HEW AND COMPUTERS

In July of 1976, the Department of Health, Education, and Welfare was asked to give the Senate Government Operations Committee information about its computer operations. On August 18, 1976, William A. Morrill, Assistant Secretary of HEW for Planning and Evaluation, submitted a "draft testimony" to the committee in response to specific questions the committee staff had raised regarding HEW computer operations, including what steps the Department had taken to improve computer security and control computer-related crime.

In response to these questions, Assistant Secretary Morrill said HEW has 163 computers. HEW's computers in fiscal year 1976 generated checks in the amount of about $84 billion, Morrill said.

Morrill said computer-generated check disbursements on a program-by-program basis in fiscal 1976 could be categorized this way:

Agency	Program/function	Amount (billions)
Department of Health, Education, and Welfare.	Federal assistance financing system (payments to recipients).	$2.5
	Central payroll	2.5
Social Security Administration	Retirement and survivors insurance	62.1
	Disability insurance	9.2
	Black lung	1.0
	Supplemental security income	5.7
		Millions
National Institutes of Health	Expense	$88.5
Office of Education	Basic educational opportunity	5.0
	Guaranteed student loan	247.0
	School assistance in federally affected areas	427.0
	Indian education	23.0

Morrill said HEW and its components operated computers in Washington, D.C.; Lexington, Ky.; Atlanta; Morgantown, W. Va.; Cincinnati; Salt Lake City; Raleigh, N.C.; Albuquerque; New Orleans; Baltimore, Rockville, and Bethesda, Md.; Miami; Birmingham; Chicago; Kansas City, Mo.; New York City; San Francisco, and Philadelphia.

Morrill said that, besides the $84 billion in checks processed through HEW computers in 1976, the entire departmental ADP budget exceeds $350 million. Morrill said computers and associated technology "play a very important role in the operations of HEW."

In light of HEW's large investment in computers, and with computers processing $84 billion in HEW checks, the committee staff sought to determine the capability of the Department to investigate computer-related crime. Accordingly, the Department was asked how many investigators it had who were trained to work on cases regarding ADP abuses. Morrill said that the Department had no investigators trained in investigating computer crime. However, he said, HEW was initiating action to develop computer-related criminal training for its investigators.

Morrill said:

> It is the Secretary's [David Mathews] intention and personal commitment to insure that the Department exercise its full capability to prevent, as well as detect and investigate, program fraud and abuse. The responsibility to build an effective and ongoing monitoring process to assess, minimize, and prevent the possibility and occurrence of program violations rests with the agencies. However, we recognize that program integrity is a continuing critical institutional responsibility of this Department.
>
> In order to meet this responsibility, the Secretary created the Office of Investigations to detect and investigate program fraud and abuse, and also assigned the responsibility

> for computer security to the Deputy Assistant Secretary, Management Planning and Technology [Thomas S. McFee].
>
> The Office of Investigations, which reports directly to the Under Secretary [Mrs. Margaret Lynch], was formed to combine departmental criminal investigative expertise into one high-level office.
>
> The Director of the Office of Investigation, John Walsh, has the authority to undertake investigations of alleged cases of malfeasance, fraud, misuse of funds, equipment, or facilities, violations of terms or conditions of funding, and conflict of interest by employees, grantees, contractors, and other personnel working on behalf of the Department. No other unit or official within the Department may undertake such investigations unless specifically authorized by the Director, Office of Investigations.
>
> . . . Currently, the Office of Investigations has no investigative personnel with computer fraud training. We have, however, made arrangements with the Federal Bureau of Investigation to obtain computer-related fraud training. The FBI has prepared a special 1-week course for OI [Office of Investigations] investigators covering the areas of investigative techniques for computer crimes. We estimate that 20 to 25 of our key personnel will attend this session at the FBI Academy, Quantico, Va., from September 27 through October 1, 1976. In addition, we anticipate that by January 1977, we will send selected key personnel to various civil service schools relating to computer security.

On December 6, 1976, John Walsh, Director of the HEW Office of Investigations, was asked by the committee staff if department investigators had begun to enroll in the courses in computer training, as planned. Walsh said the HEW criminal investigators were taking the courses in computer training on schedule and that several agents had told him that they felt they had benefited considerably from them.

The department was asked to describe the extent to which computer-related fraud had been detected in HEW programs. Morrill said the Office of Investigations at HEW "is aware of 14 instance of computer-related crimes." By "instances" Morrill apparently meant individual violators as he went on to explain that of the 14 "individuals," 8 were indicted and 6 have been convicted. Morrill said their sentences ranged from 1 to 2½ years' incarceration. Two persons fled after being indicted, Morrill said, adding that the remaining six cases were still under investigation. Two of these six cases have been referred to the Justice Department, Morrill said.

Morrill said HEW's experience with computer-related crimes had supported the conclusion of the General Accounting Office that violations in Federal ADP programs were more often the work of lower level employees with a relatively limited knowledge of computer technology. Morrill said violators tended not to have senior positions and compromised the computer system by feeding false information into it. They hoped to profit by having the computer initiate actions that would result in checks being written to them personally, to them under an assumed name or in the name or account number of an accomplice, Morrill said.

Morrill cited one instance in which an employee of an insurance company under contract to HEW gave a Federal computer program false information regarding medicaid. Morrill said the woman fed the machine bogus data so that the computer would generate medicaid checks to herself and her accomplices.

In another case described by Morrill, a social security employee found that a social security beneficiary had been overpaid. The employee had the beneficiary write him a personal check to cover the overpayment. The social security employee endorsed the check and deposited in into his own bank account, Morrill said. The employee then entered a waiver of this overpayment into the computer, Morrill said.

HEW has taken steps to control computer-related crimes, Morrill said. John Ottina, Assistant Secretary for Administration and Management, and John Young, Assistant Secretary, Comptroller, issued joint instructions to the component organizations of HEW directing them to (1) identify those computer-based asset management or control systems under their jurisdiction which are most susceptible to computer-related crimes; (2) conduct an internal review of the internal control practices for each system identified as being susceptible to computer crime; (3) verify the existence of necessary controls to preclude the misuse of computer resources; and (4) report to Assistant Secretary for Administration and Management Ottina the results of each review and corrective action taken.

The Department was asked to review its audit operations. The committee staff asked to what extent audit personnel were trained to detect potential fraudulent situations and what procedures auditors followed when they noted an irregularity which could be fraudulent. Did auditors, for example, work in coordination with HEW criminal investigators?

In reply to the question of how effectively HEW criminal investigators worked with HEW auditors, Morrill said the two offices worked together successfully.

But to make certain no difficulties arose between the investigative and audit functions at HEW, the Under Secretary of HEW, Margaret Lynch, had, on January 15, 1976, issued a memorandum directing that the Office of Investigations request any assistance required from the HEW Audit Agency in carrying out fraud inquiries. Morrill said any conflicts over requests for audit assistance were to be brought to the immediate attention of the Under Secretary.

In turn, the memorandum went on to say, should the HEW Audit Agency discover any indication of fraud the Office of Investigations was to be informed within 24 hours. "No discovery of fraud or allegations of fraud shall go unreported or undocumented as to final disposition," Under Secretary Lynch said in her memorandum.

Morrill said that when the HEW Office of Investigations gathers evidence sufficient to demonstrate that a computer fraud has been performed, the Department of Justice is contacted "for proper resolution of such matters." These procedures are followed at HEW in areas of alleged fraud in noncomputer cases as well, Morrill said.

As for the Department's policies regarding the auditing of computer systems, Morrill had this to say:

The HEW Audit Agency's role to date in auditing computer related abuse—with a few exceptions and for key management systems—has been to evaluate the (i) extent of compliance with established policies and procedures, (ii) reliability of data produced by a system, and (iii) adequacy of internal controls. Regarding the latter, when we review internal controls our objective is to verify that the system fixes responsibility, assures accountability at every level, and minimizes opportunities for fraud and abuse.

One recent example of our reviews of program functions either supported by or operated through computer-based data processing systems is our report on the supplemental security income (SSI) program. We found that the analysis, design, and computer programing functions and operational functions for the SSI program were performed by the same group. As a result, we reported, "when the same staff develops computer programs and his complete tape files and operating facilities normal internal control safeguards are not operative and the risk of systems fraud and manipulation is substantially greater." We have also issued reports covering computer applications on the student financial aid programs in OE, the civilian payroll in HEW, and the medicare program as administered by various intermediaries.

There are some who believe the auditor should go beyond his traditional role and actively participate in the design of computer systems or modifications prior to their implementation. They argue that to have auditors involved at the start during design would preclude expensive and time-consuming revisions which may be recommended later on. However, we do not have, at this time, the numbers of staff with the expertise required to actively participate on a full-time basis in the design of computer systems. We favor a more limited review of such systems or modifications prior to their implementation to assure that necessary internal control and audit trial features have been adopted. In this connection, we are currently exploring ways to improve communications with offices involved in systems development so that our staff are routinely advised when system modifications are planned.

Auditing standards call for the review of internal control features of an organization as a necessary and important part of the audit process. As mentioned earlier, internal control systems, if properly designed, serve to minimize opportunities for fraud and result in its early detection if it occurs. Our professional audit staff is qualified to review this important area with respect to computer-related operations. Qualifications are derived from training and on-the-job experience as well as from educational background.

In addition, the Audit Agency employs a new and innovative "auditing through the computer" technique which we call the HEW Computer Auditing System (HEWCAS). By using HEWCAS our auditors can extract needed audit data directly from computer files. This accessibility gives the auditor a greater chance to detect fraudulent conditions should they exist. HEWCAS in-house training has been provided to 457 of our professional staff of around 850. Each of our 10 regional offices has 1 or more HEWCAS "specialists" who determine when and how HEWCAS applications can be made. Finally, 178 of our staff have had other training in computer-related areas at both Civil Service Commission-sponsored courses and at colleges and universities.

HEW Inspector General Is Created

Between the time when Assistant Secretary Morrill submitted his statement to the committee and the issuance of this staff study, an important development occurred that may improve HEW's ability to detect and investigate computer crime and manage its ADP operations with increased efficiency and economy.

That development was the creation of an Office of the Inspector General at HEW. Assistant Secretary Morrill's statement for the committee was dated August 18, 1976. On October 15, 1976, President Ford signed into law H.R. 11347, legislation to establish within HEW an Office of the Inspector General to conduct and supervise audits and investigations relating to the Department's programs and operations.

The bill, Public Law 94–505, calls for the Inspector General and a Deputy Inspector General to be appointed by the President and with the advice and consent of the Senate. It is the intent of the bill that, while the Inspector General and the Deputy Inspector General are to serve at the pleasure of the President, they are to be selected not according to political considerations but on the basis of proven competence and integrity.

The Office of the Inspector General is to absorb the authority and duties of both HEW's Auditing Agency and its Office of Investigations. In turn, reporting directly to the Inspector General will be an Assistant Inspector General for Auditing and an Assistant Inspector General for Investigations. Both Assistant Inspector General positions are to be selected by the Inspector General after appropriate Civil Service procedures. The Office of the Inspector General will be under the general supervision of the Secretary of Health, Education, and Welfare but will be expected to report to the Congress annually. The Office will have subpena power.

Legislation to set up the Office of the Inspector General at HEW was reviewed in the House of Representatives where the Committee on Government Operations issued a report on HEW entitled, "Prevention and Detection of Fraud and Program Abuse."

In the report, filed January 26, 1976 by Chairman Jack Brooks of Texas, the committee issued a series of findings and conclusions. The findings and conclusions were arrived at in light of the committee's consideration of legislation to set up the Inspector General position at HEW. But the findings and conclusions also have application to the subject of this section of this staff study, for the House committee report cast doubt on the ability of HEW, as then organized, to control, detect and investigate fraud, mismanagement, and irregularities in any of its programs, be they computer-related or not.

Here is what the House Committee on Government Operations said:

> (1) The Department of Health, Education, and Welfare currently is responsible for about 300 separate programs involving expenditures in excess of $118 billion annually—more than one-third of the entire Federal budget. Because of the magnitude and complexity of its activities, aggravated in many instances by lack of direct control over expenditures, HEW's operations present an unparalleled danger of enormous loss through fraud and program abuse.
>
> (2) HEW officials responsible for prevention and detection of fraud and abuse have little reliable information concerning the extent of losses from such activities.
>
> There is no central source of data concerning fraud and abuse nor, evidently, has any meaningful attempt been made to evaluate the overall extent of the fraud and abuse problem. Statistics which are available are often incomplete and unreliable.
>
> HEW officials were unable to provide such basic information as an accurate count of the number of HEW programs until more than 5 months after the information was initially requested. During this period, at least four different figures on the number of HEW programs were supplied to congressional committees, ranging from a low of 250 to as many as 320.
>
> Without adequate information, neither HEW officials nor Congress can accurately measure either the need for or the effectiveness of action to prevent and detect fraud and program abuse, nor can priorities for use of available resources be determined on a rational basis.
>
> (3) Fraud and abuse in HEW programs are undoubtedly responsible for the loss of many millions of dollars each year. The committee has not attempted to name a specific figure at this time because HEW officials could not provide information on which a reliable estimate of such losses could be based.
>
> (4) HEW units charged with responsibility for prevention and detection of fraud and program abuse are not organized in a coherent pattern designed to meet the overall needs of the Department.
>
> There is no central unit with the overall authority, responsibility, and resources necessary to insure effective action against fraud and abuse. Under its charter, the Office of Investigations and Security has departmentwide responsibility for leadership, policy direction, planning, coordination, and management of investigations. However, its authority over operations of the Social Security Administration has been effectively nullified as the result of agreement made by non-OIS officials; moreover, OIS could not possibly carry out its assigned responsibilities with the hopelessly inadequate resources it now has.
>
> Fraud and abuse units other than OIS and the audit agencies are scattered throughout HEW in a haphazard, fragmented, and often confusing pattern. Some major programs

have no fraud and abuse unit, while other units exist mostly on paper. Some units have no personnel in field offices; in other instances, field personnel are not subject to the direction and control of the unit's headquarters. Personnel of most units work exclusively and continuously on a single program, and are not available to help correct more serious problems elsewhere.

(5) Personnel of most HEW fraud and abuse units lack independence and are subject to potential conflicts of interest because they report to officials who are directly responsible for managing the programs the unit is investigating. Under these circumstances, employees may be inhibited in making an honest and thorough report that could embarrass their superiors.

The independence of the Office of Investigations is restricted in another way. Under current arrangements, OIS may not initiate any investigation without specific approval of the Secretary or Under Secretary. In addition to the obvious restriction on the independence of OIS, this procedure creates an unnecessary burden for the Secretary or Under Secretary and places them in the undesirable position of having to decide personally whether or not suspected irregularities are to be investigated. Any safeguards necessary to insure that inappropriate investigations are not conducted should be imposed through carefully adopted procedures and guidelines, rather than individual decisions by the Secretary or Under Secretary.

(6) Under current organizational arrangements, there is little assurance that the Secretary will be kept informed of serious fraud and abuse problems, or that action necessary to correct such problems will be taken. The OIS charter does not provide for guaranteed access to the Secretary or Under Secretary. Most other fraud and abuse units report to program officials, usually at a relatively low level. Since those receiving reports of fraud and abuse problems are likely to be responsible for the programs involved, there may be little incentive for such officials either to call problems to the attention of the Secerteary or to initiate prompt and aggressive corrective action which could result in public laundering of their own dirty linen.

(7) Resources devoted by HEW to prevention and detection of fraud and program abuse are ridiculously inadeqaute. Although HEW has more than 129,000 full-time employees, the Office of Investigations and Security has had only 10 investigators.

At least partially because of its fragmented organizational structure, HEW has failed to make effective use of the resources it has. As a result, OIS has a 10-year backlog of uninvestigated cases; at the same time, the 11 investigators in the SSA Investigations Branch have been so underutilized that the unit has no significant backlog and has left eight investigative positions unfilled.

Although the total number of persons reported assigned to fraud and abuse units is about 300, more than 180 of them work exclusively on the medicare program, and most of the remainder are assigned to other programs of the Social Security Administration. Individuals working in OIS and the SSA Investigations Branch are qualified investigators, but personnel assigned to other units may have no substantial investigative training or experience.

8. There are serious deficiencies in the procedures used by HEW for the prevention and detection of fraud and program abuse. Until recently, HEW had not advised employees of the Department that they had an obligation to call information indicating possible fraud or abuse to the attention of appropriate officials. Moreover, there is no departmentwide policy for or centralized supervision of the referral of possible fraud cases for prosecution.

The subcommittee's investigation disclosed instances in which it took as long as 5 years or more for HEW to take corrective action after deficiencies in its regulations became known. Part of the blame can be attributed to cumbersome procedures for changing regulations; however, some delays were so lengthy as to indicate the almost total lack of any sense of urgency.

HEW Review of Computer Crime Issue

In the spring of 1976, the U.S. General Accounting Office issued three reports to Congress on computer problems in Federal programs. The third of these reports came out May 10, 1976. Also on May 10, Senator Ribicoff, chairman of the Government Operations Committee, announced in Senate remarks that he had directed a preliminary staff investigation to follow up on the three GAO reports.

On May 18, 1976, Senator Ribicoff wrote to David Mathews, the Secretary of the Department of Health, Education, and Welfare, to advise him of the committee staff's preliminary inquiry, request his Department's cooperation and make known the committee's interest in learning how HEW was coping with the problem of computer-related crime.

On June 8, 1976, a review was begun at HEW of all activities which are vulnerable to computer crime. The review was also aimed at arriving at a series of recommendations for corrective action which would reduce an activity's vulnerability to computer abuse.

On June 10, 1976, the staff of the Senate Government Operations Committee advised HEW of its interest in receiving from the Department any review of activities found to be vulnerable to criminal exploitation through computer abuse.

William A. Morrill, Assistant Secretary of HEW for Planning and Evaluation, submitted the Department's overall presentation on computers to the committee August 18, 1976. In that presentation, Merrill said the results of the ADP review would be made available to the committee by November 8, 1976.

On December 6, 1976, the committee received from the Department a copy of the review. The HEW document, which is also dated December 6, 1976, is entitled "DHEW Computer-Related Crimes Review."

The review follows:

Management Summary

In a memorandum issued jointly on June 8, 1976, the Assistant Secretary, Comptroller, and the Assistant Secretary, Administration and Management directed organizations in the Department to: Identify their systems that are potentially vulnerable to computer-related crimes as defined in the April 21, 1976, GAO report: highlight the major reasons where weaknesses exist; verify the existence and adequacy of control practices; and define the remedial actions that are under way to reduce the risk of fraud. This report summarizes the responses received to that memorandum.

As was expected, organizations generally identified those systems which processed financial transactions leading to disbursements of public funds as being most susceptible to computer-related crimes. Most organizations were sensitive to the need to safeguard personal data and to prevent its use for personal gain. Some organizations commented on the need for measures to minimize the risk of computer resources being used for personal purposes or gain.

The major reason advanced by several organizations for potential computer-related crimes was the capability of individual employees to introduce fraudulent records and transactions into a system which would produce a payment that would go undetected for lack of internal system controls.

In some cases this could be done by one individual; in other cases collusion would be required. The 14 cases of computer-related crimes investigated by the DHEW Office of Investigations involved employees who entered fictitious names and false transactions in their respective systems to generate fraudulent payments.

Various control measures to minimize the risk of computer-related crimes were described by organizations. Separation of duties appears to be the most widely-used technique. All reporting organizations recognized the need for strengthening existing controls or instituting new controls including techical safeguards in systems design and in computer programs. Remedial actions underway are in various stages of development or implementation. These remedial actions will be monitored by the Office of the Secretary, DHEW as a part of its on-going program to improve ADP system security in the Department.

DHEW DEPARTMENTAL SYSTEMS SUSCEPTIBLE TO COMPUTER-RELATED CRIMES

Departmental Personnel and Payroll Systems

The Department operates a centralized personnel data system and a payroll system which receives input data from servicing personnel offices and time and attendance supervisors throughout the department. These systems have been identified by the Deputy Assistant Secretary, Personnel and

Training of the Department as being vulnerable to computer-related crimes.

The capability for introducing fraudulent data into the personnel and payroll systems is real and could possibly go undetected for a considerable period of time due to a lack of audit features in existing personnel and payroll computer programs.

As in any personnel and payroll system, there is the possibility that a person having access to the files will sell personnel or payroll information or accidentally disclose personal data. The terminals used to input data into the personnel and payroll systems are vulnerable to use by unauthorized persons or use by authorized persons for illegal purposes.

The Deputy Assistant Secretary, Personnel and Training has identified actions necessary to deal with the type of problems described above and has established an internal management committee to insure that recommended actions are completed. The principal actions planned are:

(a) Pay and personnel records of employees will be periodically audited to detect discrepancies between authorized and actual data records. An audit sample from the master file will be reviewed at least 4 times a year.

(b) The HEW Audit Agency will be requested to assist in developing better audit trails and controls in existing and/or proposed systems.

(c) Servicing personnel offices will be required to establish controls over keying and receipt of documents that will insure integrity in operations.

(d) Servicing personnel offices will periodically verify master file data to insure that discrepancies on key items such as service completion data do not exist.

(e) Changes to all computer programs will be strictly controlled by a supervisor of programing. He will review program runs periodically to insure that no unauthorized changes have been made.

(f) Lockout devices will be provided in all programing.

(g) Terminals will be located in a room that can be secured. Doors to terminal rooms will be locked at all times.

Departmental Finance and Accounting Systems

Departmental finance and accounting systems that have been identified by the Office of the Comptroller as susceptible to computer-related crime include: the Departmental Federal Assistance Financing System (DFAFS); the Regional Accounting system (RAS); the Office of the Secretary, Direct Access Accounting System (DAS); and the Central Registry System (CRS).

The DFAFS is the departmental system through which letters of credit and Treasury checks are issued to State governments and other grant recipients for the financing of grants awarded throughout the Department. While all departmental grants are not yet processed through this system, the dollar volume is substantial. Since DFAFS is a major departmental disbursement system which receives input from the other four systems listed above as a basis for its outputs, the Comptroller subjected it to intensive analysis and is planning several actions to reduce the vulnerability of the system to computer-related crimes.

DFAFS is a relatively new system with start-up problems inherent in any new system. Since the original design of DFAFS did not include output data necessary to establish a general ledger—or data necessary to establish controls over payments made by the system—the possibility exists to commit fraud.

Present Controls Within the DFAFS System

Authorization

There are strict prohibitions against DFAFS personnel inputting authorization transactions or corrections with the exception of input for the Social Security Administration (SSA) and the Environmental Protection Agency (EPA). These are entered by a specific accounting technician under the review of the Chief, Accounting Section.

Payments

Batch controls over letters of credit have just been put into operation, as well as those cash request payments which may be made through the automated processes of the system.

Additionally, there is a separation of duties, that is, the personnel responsible for the system input of payments are not the same personnel who monitor the cash in the hands of the recipients. A new report, "Advance Greater Than Authorized," which has just been made operational will be used to aid in the monitoring of recipient cash advances exceeding authorization.

Systems manipulation ad unauthorized use

DFAFS had no control over this in the past. The system support was provided by an outside source. However, when the new DFAFS systems function is fully staffed, provisions will be made to monitor system abuse.

Returned checks

The only control exercised presently over returned checks is the maintenance of a manual log upon receipt of the check.

Proposed Controls Under Consideration by the Comptroller

Authorization

(1) Require the principal operating components (POC) to synchronize their systems with the authorization data in DFAFS' and certify thereto.

(2) Have the system produce authorization input and output totals, so that DFAFS staff may validate the authorization, as well as detect any loss of authorization by the system.

Payments

(1) Once again have the system provide input and output totals necessary to insure control over payments and to signal the loss of any information from the system. DFAFS system

controls are being developed now and are scheduled to be operational by December 31, 1976.

(2) Establish a general ledger in DFAFS.

Systems manipulation

(1) Establish periodic checks by Chief, DFAFS, into computer usage time.

(2) Require the systems chief to monitor closely all programs being written by his staff, as well as the usage of the computer facilities.

(3) Require the systems chief to develop a model to assess vulnerability of DFAFS to perpetration by fraud.

Returned checks

(1) Have the mail clerk establish a log of all checks received, in addition to the one currently being maintained by the DFAFS payment section. Compare both logs periodically.

In summary, while the Comptroller has identified five major departmental systems which are susceptible to computer-related crimes, he is concentrating his remedial efforts initially on the disbursement system, the DFAFS, which is involved in the issuance of letters of credit and treasury checks to State governments and grant recipients for the financing of grants awarded throughout the department. Since DFAFS interfaces with the other four systems, improvement of controls within DFAFS will reduce the susceptibility of the other systems to computer-related crimes.

Department of Health, Education, and Welfare Principal Operating Component Systems Susceptible to Computer-Related Crimes

Education Systems

The Assistant Secretary for Education (ASE) has identified the following systems in the Office of Education (OE) as being vulnerable to computer-related crimes: the OE financial management information system (OEFMIS); the basic education grants system; and the guaranteed student loan system.

The OEFMIS System

The OEFMIS system supports the operation of the Finance Division in OE under DHEW's umbrella accounting system. OEFMIS receives accounting data from the regional accounting system, the guaranteed student loan system, the basic education grants system, and the Indian program system. The OEFMIS does not write checks automatically but it does create transactions where payments are made. The potential for fraud exists in the OEFMIS environment through collusion and through the generation of fictitious data. This possibility is particularly evident in the grants area and in contracting where in many cases the office that authorizes the grant or awards the contract is also the same office that administers payments.

The OE Finance Division is taking the following action to strengthen established controls and develop new procedures to reduce the potential opportunities for computer related crimes:

(1) An organization plan will be developed by the systems manager that will segregate the duties of individuals to minimize their opportunity to misuse or misappropriate resources.

(2) Concurrently, an established system of practices will be developed for each duty and function. These procedures are scheduled to be completed no later than December 31, 1976.

(3) During fiscal year 1977, five major enhancements are planned for the OE Financial Management Information System: development of an audit trail; an accounts receivable system; online fund control; reduction of files; and modification of current report formats. These enhancements to OEFMIS will develop a system of authorization and record procedures.

Basic Education Grants System

OE has identified several areas for potential fraud in its Basic Education Grants System.

Although they represent areas that are susceptible to fraud, there are control procedures in the existing system. These controls are:

(a) Annual "validation rosters" submitted to the schools for verification of awards are reconciled to the progress reports submitted by the respective schools.

(b) Authorization letters are forwarded to schools indicating increase or decrease in funding levels.

(c) A production control coordinator accounts for all input and output tapes used in production.

(d) The operations at the student application center makes processing of fraudulent applications difficult.

(e) The OE Program Information and Monitoring System (PIMS) has a reasonableness check program, entity number checks and production control checks to preclude minor fraud. A recent change in maintenance contractors minimizes knowledgeable contract programmers from perpetrating fraud.

OE is analyzing financial vulnerability in this system and is giving priority to improving financial controls. OE has initiated action to verify accuracy of data on student applications forms, on a sampling basis. OE is planning to compare educational grants to the student record and to other student financial aid transactions to verify authenticity of the student and the amount of the award. OE will install new audit trails, new controls, new balancing procedures and thorough reconciliation procedures. OE has recommended that the HEW Audit Agency review the proposed revised procedures for appropriate financial control. OE is installing an independent tracking system that will identify all obligations or deobligation transactions and report items for research.

Guaranteed Student Loan System (OGSL)

The Office of Guaranteed Student Loans processes claims payments through the OGSL claims system and the OGSL collection system. OGSL is using a real-time computer system. Data is entered through remote terminals by authorized personnel from the 10 OGSL regions and national headquarters in Washington directly into the computer in Pittsburgh.

Claims Processing

Computers mail applications for insurance claims on Federal insured student loans to the servicing regional office for claims in default. When the regions receive claims, they are reviewed and then entered into the computer system, which prints out a "Claims Review Sheet" the next day. This is given to a claims examiner who studies it and approves some of the claims for payment and requests information or corrections on others. Information on the approved claims is then entered into the system. Corrections are made to the other claims until they are approved or rejected.

A magnetic tape of approved claims is produced in Pittsburgh and mailed to OGSL, as the authorization needed for Treasury to produce checks to the lenders.

The Claims Examining Group is responsible for reviewing the claims file for all claims accepted by the computer. This review is the final determination as to whether the claim is approved for payment or rejected and returned to the lender.

There are measures taken to identify fraudulent claims. Since all Treasury checks are sent to an approved lender (banks and schools) in its name, and since the lender originates the claim and receives payment, it is possible to have a fraudulent claim payment. However, the original loan application will have a time-date stamp from Norfolk. This stamp is only available in Norfolk; the regions do not have it. Should a fraudulent claim come in from a lender, the absence of the stamp will alert the mail clerk, the terminal operator, and the claims examiner.

Payment Processing in the OGSL Collection System

Student borrowers mail installment payments to the regional office. to satisfy a repayment agreement for a defaulted federally insured student loan. Incoming payments are most commonly in the form of personal checks, money orders, certified checks, or cash.

To reduce the possibility of loss or destruction of payment during processing, all borrower payments are Xeroxed. The actual payment instrument is filed and the copies are sent to data entry for processing and acknowledgment of receipt.

Control totals are manually checked for both the original instruments and the copies. These controls are maintained throuhgout the manual and computer process to provide a clear audit trail, fiduciary accountability, and accurate management control.

As the procedures show, three people in each region handle identical check transactions. Their functions are audited and periodically reviewed by supervisors. It would require collusion on the part of several people reporting to different supervisors before funds could be diverted.

The computer room is locked to all outsiders. The system is monitored during the day and occasionally in the evening. All authorized personnel have their own account number which is readily identifiable by the other users. In order for the user to get access to his account, his unique password is required.

The master files within the OGSL systems are reasonably safe from tampering by personnel in the regions and in the central office due to the fact that each master file has its own unique password which must be entered in order to change, add, or delete a record. These passwords are known only by certain key OGSL employees in Washington, D.C., and their counterparts at the contractor's office, and are changed whenever a key person leaves the project.

Currently, each region has its own password to sign onto the computer system. Each region can choose and change its password when required to do so, such as when personnel leave.

Partly due to the large personnel turnover in the regions, the security of the computer system is to be strengthened in the following manner: The regions will continue to have their own password so that one region cannot read another's data, but the central office will assign the passwords and change them at least bimonthly within a different time frame. The branch chiefs and one of their employees will be the only central office people who will know the passwords and will be responsible for informing their counterparts in the regions of the changes.

PUBLIC HEALTH SERVICES SYSTEMS

The Office of the Assistant Secretary for Health (OASH)

The Office of the Assistant Secretary for Health (OASH) identified the Public Health Service (PHS) manpower data system as being susceptible to criminal activity. This system provides PHS personnel related information to the DHEW personnel data system. The system has been modified to include passwords and limited access. In addition, the backup material and printouts are secured in locked files and rooms.

Health Resources Administration (HRA) Systems

A review of the Health Resources Administration National Center for Health Statistics (HRA NCHS) disclosed a need for improved security procedures in handling input data. A review of these procedures is continuing to identify and implement improvements. Another deficiency that was discovered and corrected was the inability to produce a record showing who had access or potential access to data, file, and equipment, particularly with regard to visitors to the NCHS installation.

Most outputs from HRA systems are subject to objective reviews by program officials, who are not involved in data manipulation. When necessary for data protection, programing technology is used to imbed coding requirements to which the user must respond in order to continue or complete certain actions. Without the knowledge of such coding, the user is stymied. If necessary, HRA has the added facility to encode information. Generally speaking, because of the nature and use of the agency's information and ADP operations, altering or destructive actions would not result in monetary loss, if any, to the Government or significant personal gain for the perpetrator.

The HRA review did not identify any specific ADP system as being susceptible to computer-related crimes as defined in the GAO report. However, practically any ADP system which may be accessed by a communications terminal is susceptible to the GAO crime category of "unauthorized or inappropriate use of facilities and supplies." Some security is provided by the need to use access control items, such as valid telephone number, authorized user identification codes, keywords, and an output location code. Complete knowledge of these items is normally difficult to obtain. An unauthorized user would probably be detected as a result of management's review of weekly control reports which reflect user activity.

The Center for Disease Control (CDC) Systems

CDC's review identified the national occupational health survey data projection system and the coal miner medical information system as being the most susceptible to criminal activity.

CDC's security measures include: (1) door locks in the computer area; (2) written procedures for handling and processing data; (3) passwords to gain access to restricted or "privacy" data; and (4) passwords for utilizing remote terminals.

Alcohol, Drug, Abuse, and Mental Health

The Alcohol, Drug Abuse, and Mental Health Administration's (ADAMHA) physical security resides with the Parklawn Computer Center (PCC), a division of the Food and Drug Administration. PCC maintains practically all of ADAMHA's magnetic tape reels and disk packs. Security measures prevail for the equipment that is used in ADAMHA. Computer crime per se does not comprise a major threat to ADAMHA as financial data disbursements are handled elsewhere in HEW.

All files are safeguarded through the use of software labels which appear on magnetic tapes and in the data set name on disks. All interactive systems require passwords to permit sign on. The unauthorized use of remote terminals in ADAMHA offices is fairly well guarded through these procedures.

Control for the misuse of computer resources is managed through accounting procedures. Each month the ADP center supplies ADAMHA with accounting information including a list of every job submitted and run during that period. Each job is identified as to the submitter, the organization (within ADAMHA) requesting the job, the date and time of day, and costs involved. This plus the PCC's own traceback routines provide a running account of ADAMHA's use of PCC facilities. The same procedure also traces possible unauthorized use of the PCC facilities by outsiders.

National Institutes of Health

The National Institutes of Health (NIH) took the following actions to evaluate the security of the NIH ADP systems against computer-related crimes.

The NIH annual ADP plan, which contains an inventory of the NIH computer applications, was reviewed and a number of high risk ADP applications identified.

The NIH program officials responsible for these ADP applications have been directed to review the security of their applications against computer-related crimes. General guidelines for the reviews have been furnished to the program officials and they have been instructed to report the results of their reviews to an independent group at NIH. This independent group will evaluate these reports and make tests to determine if internal controls are adequate to secure these ADP applications against computer-related crimes. NIH plans to continue this type of internal review until all high risk ADP applications have been reviewed. In addition, the review of the physical security of the NIH computer facility has been assigned to the Division of Computer Research and Technology, NIH, and their report will also be evaluated by the NIH independent group.

Further, NIH has indicated plans to conduct these reviews on a cyclical basis so that the security of NIH ADP applications will be under continuous scrutiny.

Health Services Administration (HSA)

The Health Services Administration (HSA) evaluated four areas which have potential for criminal actions. It was determined that the probability of criminal actions being attempted is very low. Most of the HSA systems contain routine medical and administrative data which has very little value outside of HSA. Since medical data has always been treated as confidential, only one system was found to require additional security measures (locked cabinets are now being used to store data for that system).

Food and Drug Administration (FDA) System

The Food and Drug Administration (FDA) evaluated ADP systems which may be susceptible to unauthorized access, FDA reported that it found no instances of falsified data input, unauthorized equipment usage, alteration or destruction of data, or unauthorized access of data.

Social Security Administration (SSA) System

The Social Security Administration (SSA) completed a survey in 1975 of computer-based systems to assess data base integrity and security. The interim report, published August 4, 1975, presents the results of security techniques used at major work areas in the SSA organizations.

SSA Retirement and Survivors Insurance

A survey of the retirement and survivors insurance area indicates that integrity and data security need improvement.

SSA Disability Insurance

The disability insurance showed a weakness in providing a written plan for physical and systems security regarding telecommunications equipment. The survey showed that about one-third of the input forms and backup files are not stored in a secure place. The survey indicated a need for housing field office telecommunications equipment in lockable rooms and establishing a security officer function in each office. It indicated a need to develop software access control features and establish security procedures for remote terminal devices and microfiche processing.

SSA Bureau of Data Processing

The Bureau of Data Processing (BDP) reported weaknesses in the following areas:

(a) A lack of consistent attention being given to performing internal operational surveys and audits.

(b) Program modifications are not installed by the use of standard clearance and review procedures.

(c) There is a need for greater emphasis for control over access to files by employees.

(d) The physical security of the telecommunications equipment is not consistent.

(e) There is no policy for a periodic internal or departmental audit of BDP processes.

SSA Auditing

At present there are a number of formal audit functions internal to SSA; in addition, there are special staffs which review nationwide and central office workflow of all organizations.

SSA Remedial Actions

The following remedial steps are being taken by the SSA. Security awareness within SSA is not as visible as it should be. Management tends rather to concentrate on design, implementation, and operation of systems with a view toward efficient and timely operation of the EDP programs. As a first step to correct this situation, the SSA systems security staff gave a systems security presentation to high level systems management within SSA. A security awareness program is being prepared by the SSA systems security staff for dissemination throughout SSA via members of the SSA systems security work group.

Because of major workloads imposed upon SSA in the last 2 years, control over the use of remote terminals, have not been rigorously enforced. Actions taken to correct this include: installation of a software lock system; developing a security matrix whose function is to only allow specific inputs from terminals of specific organizations; and the development of a comprehensive terminal oriented security system.

An attempt is being made toward developing tighter controls over program update and modification processes.

The Bureau of Data Processing is planning a periodic internal or departmental audit of the BDP processes. It is believed that this periodic audit—every 4 or 5 years—would serve as a good deterrent to ADP security malpractice.

The SSA has organized a formal ADP security staff to insure data integrity and protection in SSA ADP systems. The staff is responsible for the management and coordination of ADP systems security to include all points of entry and exit from any SSA ADP system in field and central locations. This includes security controls and manual processing in storing and disposing of vital records. It covers all aspects of control in systems design, operating procedures, auditing, programing, and authorized use of systems and systems data.

Social and Rehabilitation Service (SRS) Systems

The Administrator, SRS, has identified the SRS accounting and financial control system (AFCS) and the terminal data collection system (TDCS) as systems that may be susceptible to computer-related crimes.

The SRS accounting and financial central system (AFCS) is considered reasonably secure from computer-related crimes since there are controls, audits, and check features, such as authorized signature comparison, prior to the entry of data. The DHEW Data Management Center (DMC) supports the data processing, maintenance and operation of the AFCS.

The TDCS terminal is operated by the Division of Personnel. It is located in a physically secured room with restricted accessibility to individuals assigned to the personnel records activity. Input records are controlled by signature verification prior to entry into the terminal.

SRS is reviewing processing and control practices to insure security of the accounting and financial control system and terminal data collection system operations.

Office for Human Development (OHD) Systems

OHD has reviewed its eight ADP systems. The review indicates that none involve asset management or control functions and are not suitable candidates for criminal activity. None contain individual data with a potential for violation of personal privacy.

OMB ACTIONS

James T. Lynn, Director of the Office of Management and Budget, wrote to Senator Ribicoff on December 29, 1976, to report on actions taken by OMB in connection with computer problems in Federal programs. The letter follows:

> DEAR MR. CHAIRMAN: Earlier this year you expressed an interest in three reports released by the Comptroller General addressing problems discovered in the management of Federal ADP resources: "Managers Need to Provide Better Protection for Federal ADP Facilities;" "Computer Related Crimes in Federal Programs;" and "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government." In previous correspondence I indicated that we would initiate action to assure that agencies reviewed these reports relative to their internal operations and undertook corrective measures as necessary and that we would provide you with an analysis of the results of these actions. The committee staff has requested our analysis of agency actions for inclusion in a report the committee is planning to publish by the end of the year. Since most agencies and departments are still in the process of developing and implementing plans to address the deficiencies noted in the GAO reports I am submitting this interim report on agency actions. A more comprehensive analysis will be provided at a later date.
>
> In order to focus attention on these important issues a number of actions have been taken: OMB requested the departments and agencies to review the reports and initiate appropriate actions; the President included these issues in his management initiatives program which directed 20 of the largest departments and agencies to undertake actions for improving agency management; and we have published OMB Circular No. A-113 which requires that each agency pay continuing attention to improving the management of its ADP resources. Copies of our correspondence to the agencies have already been provided to your staff.
>
> In the area of ADP crime and security 28 of the 48 agencies that were requested to review these reports have responded. Our preliminary review of these responses indicates that:
>
> Ten agencies reported that adequate controls were designed into their systems while two agencies indicated that they plan to implement such controls.
>
> Ten agencies reported that they had an organization plan that segregates the duties of individuals to minimize their opportunity for misuse or misappropriation of resources. Two agencies indicated that they were developing such an organizational plan.
>
> Nine agencies indicated that they had a system of authorization and record procedures adequate to provide effective accounting while one agency reported that it is planning such procedures.

Seventeen of the agencies reported that they had or planned to establish an effective system of internal review and audit.

Seven of the 28 responding agencies stated that they have a management official responsible for ADP security while three agencies indicated that they were planning to establish that responsibility.

Eleven of the agencies reported that they had internal security regulations and four agencies stated that they were going to establish and publish such regulations.

In the area of automated decisionmaking our initial analysis of the 30 responses that have been received indicates that:

Twenty-three agencies reported that they have completed reviews of their ADP systems and five indicated that they are still working on such reviews. Of the 23 agencies that have completed their reviews 10 reported that they had no automated decisionmaking systems. Of the remaining 13 agencies, six reported that all actions resulting from their automated decisionmaking systems were proper, while three reported finding some improper actions for which the causes have since been corrected and four agencies found improper actions on which they are still working.

Eight of the 30 agencies that responded reported that they have either completed the development of new policies and procedures, undertaken such an effort or plan to do so. Nine additional agencies indicated that they have either completed, undertaken or planned reviews of their existing policies and procedures.

The actions identified by the agencies to improve automated decisionmaking systems, although varying widely, include improved programming criteria and documentation standards, organizational realignments, manual intervention and review, and audits.

Although it is too early to measure the full impact that these activities will have, it is evident that agency attention has now been focused on these important issues; that plans have been developed for addressing them; and that the first steps have been taken towards both identifying and minimizing or eliminating any problems. As a consequence, we are moving in the direction of improved management of ADP resources.

We will continue to monitor agency efforts in this area and take such additional actions as are necessary. Once the agencies have more fully implemented their initial plans a more thorough analysis will be provided to you.

Sincerely yours,

JAMES T. LYNN,
Director.

FINDINGS AND CONCLUSIONS

This staff study on computer security in Federal progams supports and endorses the conclusion of the General Accounting Office that the executive branch needs to improve its safeguards against criminal exploitation of and damage to automated data processing (ADP) systems.

In addition to those probem areas which were documented in the three GAO studies issued last spring, the committee staff found two areas of computer operations which are in immediate need of improved security policies and procedures.

These problem areas are, first, those concerned with the distribution of public funds, and, second, those which offer the opportunity to divert highly private or economically valuable data.

The staff finds that these two categories of computer-based operations need improvement in terms of physical security, as demonstrated in the GAO reports. But reform is also called for in terms of personnel security, an area where there have been inconsistent and inadequate policies and safeguards to insure that qualified and trustworthy individuals are selected to work on sensitive computer operations.

The staff finds that these physical security and personnel security improvements are needed in computer systems which are owned and operated by the Federal Government. In addition, computer systems and services which the Federal Government contracts to privately owned companies should be improved as well.

The staff finds that there are three categories of Federal computer operations that should be designated as critical sensitive because of the harm or loss that could result from criminal abuse, unauthorized access or manipulation of data.

These categories of computer operations are, first, those involving access to classified and national security information; second, those concerned with the distribution of public funds; and third, those offering the opportunity to divert or otherwise abuse highly private or economically valuable data.

The staff finds that the Federal Government has taken appropriate steps to insure the integrity of those computer systems which process national security data. The staff finds that there is a keen awareness in top management of Federal agencies processing classified defense and intelligence data. But there are no corresponding safeguards, standards or adequate security procedures in many Federal programs unrelated to national defense.

As indicated in the body of this staff study, numerous experts in computer technology and systems security asserted that no computer system is absolutely secure from concerted penetration attacks. Computer experts also said that computer crimes, especially those which divert funds or convert economically valuable data, are likely to become prevalent white collar crimes in the future.

The committee staff finds that the judgments of computer experts in these matters apply to computer operations which support Federal Government projects. The committee staff wishes to alert the Congress and the executive branch that Federal Government computer systems which disburse billions of dollars in assorted benefits, tax refunds and payrolls and hold economically valuable and personal data of untold value can become targets of white collar computer criminals. That is to say, Government computer-supported projects can be victimized by white collar criminals.

Until the issuance of the GAO reports and the commencement of the committee's preliminary staff inquiry, most Federal agencies have been unprepared to cope with computer crime and the threat of physical damage. For example, at the Department of Health, Education and Welfare where computer systems distribute approximately $85 billion a year under a variety of programs—programs such as medicare, medicaid, social security and student loans—there was no capability to prevent, detect or investigate computer abuse.

It was not until June of 1976 that HEW officials made an effort to pinpoint vulnerabilities in their computer systems. The results of these efforts by HEW, as reported to the committee and detailed in this staff study, show in most instances a long-term lack of basic kinds of security and audit precautions. However, because of the establishment of more effective investigative and audit capabilities, HEW is taking action to correct deficiencies.

Under the guidance and leadership of the Office of Management and Budget (OMB), each executive agency whose computer systems are involved in the distribution of funds or the processing of valuable economic and personal data should evaluate its particular vulnerabilities and invest its resources to correct any deficiencies in ADP security. At this writing, OMB has advised the committee that such an effort has been initiated.

In the personnel area and in dealing with private contractors, the executive branch should reevaluate, clarify and strengthen security procedures. Regarding personnel practices, the committee staff found that there was agreement among Government officials and private computer experts that no matter how secure a computer is in a physical sense, physical security is of diminishing value if personnel procedures and controls are lax.

Robert E. Hampton, Chairman of the U.S. Civil Service Commission, informed the committee that Federal personnel involved in ADP work which is designated critical sensitive should be subjected to full field background investigations as a condition of employment.

Hampton's response to the committee made clear that the kinds of ADP operations which should carry the designation critical sensitive for employment purposes are those which have to do with national security data, with personal privacy information and economically valuable data, and with ADP systems that involve transactions that result in or affect the disbursement of public funds.

Hampton was careful to distinguish between those computer operations which can carry the designation critical-sensitive and those which are "casual or routine" in nature and, therefore, should not require the strict security standards associated with critical sensitive computer-related employment.

The committee staff agrees with Chairman Hampton's position in this regard and finds that in applying both physical and personnel security improvements to Federal computer systems a distinction should be made between those duties which carry the designation critical sensitive and those whose purpose and functions do not require such designation.

Chairman Hampton said that the Civil Service Commission, at the committee's request, had contacted several agencies which have major computer facilities and found "that these agencies have not designated computer-related positions as critical sensitive for the most part; this means that a preappointment full field investigation is not a requisite for employment. The notable exception is DOD where multiple entry computers containing national security information necessitates critical sensitive classification for users."

The committee staff was assured by Defense Department and Central Intelligence Agency officials that data having to do with national security is processed in computers by persons who have been subjected to appropriate security clearances. This clearance requirement is applied to government employees as well as to employees of contractors who have access to national security data.

The committee staff found that outside the defense and intelligence realms, however, there are no personnel or physical security controls to insure that private contractors maintain standards consistent with critical sensitive computer work.

As ADP systems are used more and more by government and as more and more of these systems and related services are provided by commercial companies under contract, an increased amount of attention should be given to physical and personnel security policies in Federal programs.

The staff does not question the wisdom of the Office of Management and Budget for issuing circular A–76 directing that services, including ADP services, for Federal programs should be contracted out to private industry whenever appropriate. However, OMB circular A–76 should be revised or amended so that it gives fair and reasonable attention to the issue of computer security. Controls should exist to provide Federal agencies with reasonable assurances that the personnel working for private firms on Federal ADP projects are trustworthy and that commercial computer facilities maintain physical security standards consistent with the sensitivity of the ADP work to be performed.

The government already insists on that assurance in the awarding of sensitive national security contracts. Defense contractors and defense contractor employees must agree to submit to background checks and other personnel security controls and maintain other security standards.

But no such requirement exists in contracts issued by Federal agencies for services unrelated to national defense but which, nonetheless, are of considerable consequence and sensitivity. Contracts to commercial firms for computer services related to the disbursement of public funds, for the housing of privacy information and for the assessment of economically valuable data should contain language attesting that personnel of the contractor firms, as well as the contractor firms themselves, are suitable for government employment. The level of suitability should be commensurate with the degree of sensitivity inherent in the Federal contracts the firms are carrying out.

In his statement given the Senate Government Operations Committee, Clarence M. Kelley, Director of the Federal Bureau of Investigation, expressed apprehension about the personnel security implications of OMB circular A-76. "Those concerned with computer security in government systems," Kelley said, "should be aware that OMB A-76 which requires government agencies to obtain all services, including computer services, from the private sector whenever possible, does not permit agencies to exempt security requirements. In the computer area, just as in any other area, the level of security can only be as high as the trustworthiness of the personnel who design and operate the system. Given the transitory nature of personnel in the private sector, it is difficult to insure the reliability of all vendor personnel." The staff finds Director Kelley's concerns about the personnel security implications of OMB circular A-76 to be valid.

OMB should make it an early priority in 1977 to strengthen circular A-76 in an appropriate manner so as to allow for consistent personnel security and suitability standards whenever the nature of the computer contract is such that it can be reasonably characterized as critical sensitive.

Owing to their national security mission and the fact that this mission leads them to think in terms of securing an installation as well as attesting to the suitability of those who work there, the defense and intelligence communities have more experience in safeguarding their own ADP systems. CIA spokesman, for example, told the committee staff that they operate on the assumption that, first, a computer system can be penetrated, and, second, that an attempt will be made to penetrate it. Therefore, the CIA spokesmen said, they try to design and manage their computer systems in a way that makes a single compromise of less impact. Defense Department spokesmen gave the committee staff similar information.

CIA Director George Bush, in the statement he gave to the committee, said he did not think his organization should serve as a model for other Federal agencies in the computer security field. The committee staff agrees. But it is the staff's view that, in light of the potential for criminal compromise in the computer field, the fundamental principal defense and intelligence gathering agencies adhere to—that every system is able to be compromised; and that, therefore, an attempt will be made to achieve that compromise—has value throughout the executive branch. It is a principle all Government ADP officials should keep in mind when they set out to design, purchase, operate and manage their own non-defense computer programs.

All too often Government agencies outside the defense realm are not security conscious. As a graphic example of inconsistencies in the area of personnel security, felons incarcerated in the Federal prison at Leavenworth, Kansas were found to be engaged in computer programing functions for the U.S. Department of Agriculture. These programing functions had to do with ADP systems which are involved in the distribution of many millions of dollars in public funds. Some of the prisoner programers had relatively high rates of recidivism. Others had past connections with organized crime or had committed white collar crimes such as bank embezzlement, counterfeiting and interstate transportation of stolen or bogus securities. Several of the prisoner programers were in prison for having killed or kidnapped people or for armed bank robbery.

Based in part on the report of computer scientist and ADP security expert Robert P. Abbott of Berkeley, Calif., who served as a consultant in this preliminary inquiry, the committee staff's view is that it is an unwise policy for Federal Prison Industries, Inc., and the Department of Agriculture to have entered into an agreement whereby felons incarcerated at Leavenworth Federal Penitentiary are programing ADP systems that are involved in financial transactions.

There is no intention in this finding to in any way seek to discredit the principle of the rehabilitation of prisoners. Prisoners in Federal penitentiaries should have an opportunity to learn skills which will enable them upon release to find meaningful and productive work on the outside.

However, that being said, the committee staff finds that the Bureau of Prisons and the Agriculture Department are taking an unwarranted risk by having felons with backgrounds in bank embezzlement, counterfeiting, interstate traffic in stolen and bogus securities, murder, armed bank robbery and kidnapping, entrusted with programing computer systems that are used in financial disbursements and lending programs such as the Agriculture Department's Commodity Credit Corp. and several of the Department's farm disaster and emergency aid services.

Millions and millions of dollars are disbursed annually through these programs and the persons programing the systems that disburse these funds should be of a reasonable level of integrity. Having felons program these ADP systems is an unsatisfactory policy. It makes far more sense to have the prisoner-programmers do work for Federal agencies that offers them no opportunity to compromise Government ADP systems or gain knowledge about critically sensitive processes. It is the committee staff's view, in fact, that having imprisoned felons do government financial computer programing may in the long run cause the very concept of rehabilitation to lose credibility with the government and the public.

As computer scientist Robert Abbott observed in his report to the committee, the prisoners could do equally productive ADP work by writing programs involving data which is not related to individual privacy or the disbursement of large amounts of Federal dollars.

The irony of the peculiar Leavenworth situation is that the felons are able to write ADP programs on systems which support financial transactions while incarcerated but, owing to their felonious backgrounds, it is doubtful that they could qualify for such sensitive Federal employment once they are released.

As a result of its inquiries into the criminal cases of Leavenworth inmate Frank E. Ready, former IRS revenue official David Robinson and the Betty Marie Gholston prosecution in Detroit, as well as other information provided by the Internal Revenue Service, the committee staff finds that the IRS computerized process of auditing tax returns is vulnerable to multiple filing schemes and other tax frauds.

These schemes are initiated by criminals to "beat" the tolerance levels of IRS computers in order to obtain tax refunds. The essence of such tax frauds is the creation of false tax returns, fraudulently using W-2 forms, employer identification numbers, social security numbers and bogus items of income, deductions, depreciations and other expenses.

During the course of this preliminary staff inquiry, IRS officials worked closely with the committee staff, demonstrated their concern and took remedial actions to eliminate this vulnerability. Unfortunately, the massive volume of paper and records, plus time, cost and geographic constraints, make the total elimination of this vulnerability very difficult.

The IRS has incorporated various recommendations of an internal committee composed of representatives of each IRS component concerned with the tax fraud problem. The IRS internal group members are seeking to improve their computer systems, audit procedures and investigative techniques. These steps should increase the ability of the IRS to detect and prosecute these frauds more effectively.

At the request of IRS the steps taken by the IRS in this regard will not be detailed in this staff study.

IRS also responded to a committee inquiry regarding the feasibility of matching all W–2 forms attached to an individual return against all W–2 forms that IRS receives from employers to detect fraudulent refunds. On this subject, a report dated December 23, 1976 was written by James Owens, Assistant IRS Commissioner for Accounts, Collection and Taxpayer Services. Thomas V. Glynn, Assistant to IRS Commissioner Donald C. Alexander, forwarded Owens' report to the committee. Owens said, "We do not now check individual W–2 forms attached to tax returns against the total universe of withholding records filed with IRS by employers to assure that withholding tax credits match. Our information returns program (IRP) currently compares both income reported and withholding tax credit claimed by taxpayers with amounts reported by employers, but only a portion of the approximately 450 million information documents filed by payers of wages, dividends, interest, etc. Notices are sent to taxpayers whose income reported on the return is equal to the income reported by employers but whose withholding tax claimed does not agree with that reported by employers. Criteria indicative of refund fraud have been developed and are being incorporated in the IRP computer programs. These criteria will be applied against the tax year 1974 IRP file on a test basis and in subsequent tax year IRP matches if the criteria prove effective."

James Owens also said:

> Notwithstanding the fact that IRP does not appear to be the complete answer to stopping fraudulent refunds before they are made, this procedure may be useful in bringing to justice those who have already perpetrated such schemes. Once a complete IRP file is available for matching, we pursue leads developed by the program and our success in prosecution will hopefully be a deterrent to those who might attempt such schemes in the future.
>
> We should also mention that the Service [IRS] is now conducting a test on what is sometimes called the "reverse IRP concept." Basically, we are testing the theory that returns claiming refunds of withholdings where the Service has no record of W–2A from employers and no record of FICA wages from the Social Security Administration constitutes valid leads to fraudulent refund schemes. At this point in time, a sampling of such returns has been taken. Processing

instructions are in draft status and will be issued to our field offices shortly.

The committee has been informed that the Intelligence Division of IRS is continuing its investigation of tax fraud matters that surfaced in both the Frank Ready case at Leavenworth and the Gholston case in Detroit.

IRS is to be commended for its prompt response to issues raised in this staff study. However, the staff finds that management of security procedures and overall security awareness must be improved in the Federal Government in many other agencies.

Government users of the executive branch's largest commercial time-sharing bureau, Infonet, have been found to be careless.

The basic document on security in Federal progams, the Federal Information Processing Standard Publication 31 (FIPS-31), promulgated by the National Bureau of Standards, is vague and inadequate. Moreover, there is still no requirement that Federal agencies use FIPS-31 as even a "guideline."

Since FIPS-31 has no compliance mechanism to enforce its use, the document is not being tested and refined sufficiently to insure that one day a set of security standards for ADP programs will be adequate for governmentwide application.

In turn, the National Bureau of Standards is not the appropriate agency which should be responsible for enforcing security in Federal computer programs. NBS cannot bring to this pursuit the necessary persuasiveness to see to it that its guidelines, standards or requirements will be used, evaluated and ultimately enforced with some measure of effectiveness.

Given the present structure of the executive branch, only OMB, in coordination with the General Services Administration (GSA), can be the Federal office capable of effective leadership in this field. OMB, working with GSA, should take it upon itself to be the "lead" agency in this field, using the management authority and persuasive powers only it enjoys in the executive branch.

There is nothing new in this finding. As the staff interprets the Brooks Act and the Privacy Act of 1974 and the legislative intent of both these measures, it is the mission of OMB to be the "lead" agency in insuring that ADP systems in Federal programs be reasonably secure. It is now up to OMB to exercise that leadership. Once OMB's leadership is demonstrated, government agencies will begin the testing and refinement needed to make the FIPS-31 document workable and, to the degree possible, enforceable.

In addition, OMB can bring to this pursuit more of the resources available in the Federal Government. For example, the problem of computer security is directly related to the problem of computer crime and crimes made easier by computer technology. It is regrettable that Federal authorities are not doing more to study, understand and control computer-related crime.

Government should be more assertive in mobilizing the Nation in controlling computer crime. The Law Enforcement Assistance Administration (LEAA), which has spent billions of dollars in crime control projects including funding for the use of computers in law enforcement, has spent nothing to research the area of computer abuse to strengthen the ability of local, State and Federal criminal justice systems to cope with computer crime.

Law schools should be encouraged to train young attorneys in the computer field. Law enforcement officers should be trained in computer abuse. As many experts have informed the committee staff, all too often prosecutors do not know enough about computers to effectively prosecute crimes. By the same token, police frequently do not know enough to investigate computer-related crime. In the computer crime abuse continuum, all too often the only persons who know what they are about are the violators.

The FBI and the armed services are improving their computer abuse training programs for law enforcement officers. The Justice Department has begun to make U.S. attorneys more knowledgeable in this field.

A recent case in Baltimore involving an unauthorized penetration of Federal Energy Administration files resulted in a criminal conviction in Federal court. This conviction, although it is being appealed, has given the Justice Department increased hope that U.S. prosecutors will be able to respond effectively to computer crime cases.

However, as Richard L. Thornburgh, the Assistant Attorney General for the Criminal Division, said in his statement for this committee, the Baltimore case, encouraging as it may be, still reflects weaknesses in the government's ability to prosecute computer crime. Thornburgh pointed out, for instance, that had the defendant not used a telephone in the transmission of ADP data across State lines—from Maryland to Virginia—and had he limited his transmission of the classified data to an intrastate transaction there might not have been Federal jurisdiction, even though Federal energy records were involved. Thornburgh asserts, and the committee staff agrees, that new laws such as an expansion of the mail fraud and wire fraud statutes to include intrastate as well as interstate violations may be required.

Similarly, in response to the committee's inquiry regarding problems associated with the prosecution of computer crimes, Jervis S. Finney, U.S. Attorney for the District of Maryland, described difficulties his office faced in the prosecution of the FEA case. Finney included specific recommendations for corrective action regarding the prosecution of computer cases. The committee staff finds Finney's recommendations to be worthwhile and has incorporated them into the recommendations for corrective actions which appear in the next section of this staff study.

The committee staff also finds that Federal authorities, working in coordination with law schools and other institutions capable of conducting studies, should begin now to evaluate the criminal justice system in light of computer crime. For example, the staff finds it unfortunate that LEAA, which funds all manner of law enforcement activities—from "buy-bust" pursuits of local drug agents to the purchase of armored personnel carriers for local police departments—has not sponsored research and other efforts to enable government to cope with computer crime. It is hoped that LEAA will take an active role in this area in 1977.

In addition, the American Bar Association and other private organizations concerned with the law should initiate study programs to determine what steps can be taken in curriculum development so that more courses are taught in computer abuse cases.

No computer abuse case can ever get to trial unless it is, first of all, properly investigated. In Federal programs, criminal investigators should, at the minimum, be required to enroll in the FBI's computer abuse investigations course at the Bureau's Academy in Quantico, Virginia.

The new Inspector General at the Department of Health, Education and Welfare should see that HEW's criminal investigators continue to take this course. Investigative personnel in other agencies whose computers distribute taxpayers' money should also be required to enroll in this FBI course.

RECOMMENDATIONS FOR CORRECTIVE ACTION

The staff of the Senate Government Operations Committee, in putting forward a series of recommendations for corrective action in computer programs in the executive branch, has divided its proposals into two categories—administrative and legislative.

Administrative corrective actions are those which would not require an act of Congress. In that regard, it is the staff's view that certain computer operations within the Federal Government are in immediate need of improved security procedures and policies. This is especially true relative to those computer systems which (1) control the distribution of public funds; and (2) contain and process information which offers the opportunity to divert highly private or economically valuable data.

These two types of computer systems should be designated critical sensitive so that personnel security procedures associated with these systems can be upgraded in a consistent manner and physical security can be improved.

The Office of Management and Budget (OMB) should exercise its management responsibility with respect to improved security in Federal computer programs by taking six fundamental actions.

First, OMB should direct that executive branch departments and agencies implement the recommendations of the General Accounting Office in GAO's three reports on Federal computer operations issued in April and May of 1976.

Second, OMB should give priority to coordination of the activities of certain Federal agencies which have important functions in the improvement of computer security. In this recommendation, the committee staff has specific reference to the National Bureau of Standards, General Services Administration, the U.S. Civil Service Commission and others.

Third, under the management of OMB, the National Bureau of Standards should prepare a definitive schedule for workable physical and personnel standards to be applied by Federal agencies and private contractors consistent with the sensitivity of their particular systems.

Fourth, under the management authority of OMB, a compliance mechanism should be created to assure that these security standards are maintained by individual agencies.

Fifth, under the management authority of OMB, the General Services Administration should insure that computer-related contracts under its jurisdictions contain security requirements consistent with the sensitivity of the work to be performed by the contractor.

Sixth, under the management authority of OMB, the U.S. Civil Service Commission should be made responsible for appropriate personnel security policies consistent with computer programs that are designated critical sensitive.

In addition, those officials with security and investigative authority in Federal agencies whose computer systems either distribute public funds or contain highly private or economically valuable data should take appropriate steps to insure that their personnel are trained in the prevention, detection and prosecution of computer abuse.

Along with the above recommendations for corrective action which can be implemented by administrative direction, the committee staff wishes for Senators to also consider the feasibility of adopting three separate legislative measures. The committee staff developed these recommendations in the legislative area in consultation with representatives of the Department of Justice and other persons knowledgeable about the problems associated with the prosecution of computer crime.

There is ample evidence to suggest that much of the computer-related criminal activity has involved, or will involve in the future, government computer systems. Accordingly, consideration should be given to the feasibility of these legislative remedies:

First, legislation should be considered which would prohibit unauthorized use of computers owned by, operated for, under contract with, on behalf of or in conjunction with the U.S. Government.

Second, legislation should be considered to expand the wire fraud jurisdiction to reach any use of the facilities of wire communications, regardless of whether the actual signal travels interstate.

Third, legislation should be considered to clarify definitional guidelines as to whether checks, securities, and other negotiable instruments issued by computers in both the public and private sectors are forgeries if issued on the basis of improper or fraudulent data.

CONTINUED

3 OF 4

APPENDIX

NAVAL RESEARCH LABORATORY
WASHINGTON, D.C. 20375

IN REPLY REFER TO:
5403-289:SW:la
NRL Prob B02-25

28 JUN 1976

Mr. Fred Asselin
Committee on Government Operations
United States Senate
Washington, D.C. 20510

Dear Mr. Asselin:

Enclosed is a copy of NRL Memorandum Report 2821 that you requested from Mr. John Shore (NRL Communications Sciences Division). If I can be of further assistance, please do not hesitate to call upon me.

Sincerely,

J.T. GEARY
Captain, USN
Director

Encl:
(1) NRL Memorandum Report 2821

UNCLASSIFIED

NRL Memorandum Report 2821

Subversion of a "Secure" Operating System

[Unclassified Title]

DAVID STRYKER

Information Systems Staff
Communications Sciences Division

June 1974

NAVAL RESEARCH LABORATORY
Washington, D.C.

UNCLASSIFIED

CONFIDENTIAL, classified by DIRNRL.
AGDS of E.O. 11652.
Declassified on Dec. 31, 1974.

Distribution limited to U.S. Government Agencies only; test and evaluation: June 1974. Other requests for this document must be referred to Director, Naval Research Laboratory, Washington, D.C. 20375.

NATIONAL SECURITY INFORMATION

Unauthorized Disclosure Subject to Criminal Sanctions.

NOTICE

(U) This Memorandum Report is temporarily classified CONFIDENTIAL in order to allow the DoD installations subject to the penetration method herein described enough time to protect themselves from it. Although there exist unclassified references to the weakness in the Univac 1108 executive system which make our penetration possible, there are none which describe the covert exploitation of the weakness, and the very low cost of such exploitation is not generally realized.

(U) This document will be declassified on 31 December 1974 unless holders recommend classification for a longer period. If so, holders should furnish to NRL (Code 1240) justification for continued classification citing a specific classification authority.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER NRL Memorandum Report 2821	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) SUBVERSION OF A "SECURE" OPERATING SYSTEM (U)		5. TYPE OF REPORT & PERIOD COVERED Interim report
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) David J. Stryker		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Research Laboratory Washington, D.C. 20375		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS NRL Prob. 54B02-08 Task No. 351502-74-01
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Electronic Systems Command (ELEX 5301)		12. REPORT DATE June 1974
		13. NUMBER OF PAGES 18
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE AGDS-Dec. 31, 1974

16. DISTRIBUTION STATEMENT (of this Report)

Distribution limited to U. S. Government Agencies only; test and evaluation; June 1974. Other requests for this document must be referred to the Director, Naval Research Laboratory, Washington, D.C. 20375.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Operating Systems, Security

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

(U) This Memorandum Report describes the successful, covert subversion of a Univac 1108 Exec VIII operating system at a facility where classified and unclassified data were simultaneously resident on the system, and speculates on those aspects of the supervisor design that make penetration possible. Recommendations are made to remedy some of the faults of Exec VIII, and guidelines for the development of other operating systems are discussed.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

CONTENTS
(Unclassified)

Subversion of a "Secure" Operating System (U)

> (U) The multiprogramming capabilities of the Executive System imply that many unrelated programs may be residing in main storage at the same time. Infringement of privacy in such a mixture is highly probable, especially in cases where debugging tasks are executing. ...To combat the invasion, intentional or unintentional, the Executive System has unique features that automatically guarantee absolute program protection.
>
> Programmers Reference Manual
> Univac Publication UP-4144,
> Rev. 3, p 2-20

Section I - INTRODUCTION

(U) As the practice of online maintenance of data on multi-access computer systems has snowballed, the importance of data integrity has been recognized. The operating systems (OS) of multi-access computers normally have complete control over all system facilities, so that a breach of OS security can result in the dissemination, destruction, or modification of all data stored in the system. Any software serviced by the OS is as insecure as the OS itself.

(U) Ideally, one would like to require that OS's be absolutely secure in the sense that they never permit access to a user's data without that user's permission. A realistic requirement is that the cost of penetration exceed the value of the data gained from penetration.

(U) The Department of Defense maintains classified data on its computer systems, and believes that the cost of penetration should be correspondingly higher than is normally required on commercial systems. When several classes of users (e.g., Unclassified, Confidential, Secret, etc.) maintain data online on the same computer system, the term "Multi-level Security (MLS) System" is often used to describe the corresponding OS requirement. If an OS were completely secure, it would protect each user's data from all other users, and the division of user capabilities by the user's level of classification would be unnecessary. It is a much less stringent requirement to provide a MLS system than it is to provide a secure OS, which guarantees the data integrity of each user.

(U) We believe that penetration of most large OS's can be performed at very low costs. However, because there are few well documented

---

Manuscript submitted May 23, 1974.

examples of such penetration, there is a false sense of security among system managers, many of whom believe that holes in their systems exist in theory, but are in practice nearly impossible to exploit.

(C) The Naval Research Laboratory (NRL) has performed several tests of MLS systems; this Memorandum Report describes one aspect of a test of a MLS system operating on the Univac 1108. The OS tested was a version of the level 31 Exec VIII that was modified on site to improve its security in an MLS environment. Users were assured that their classified data was protected adequately. However, since no basic design features of Exec VIII were changed, our penetration was merely somewhat more difficult than it would have been in the case of a standard Exec VIII.

(C) Our penetration of Exec VIII was based on the insertion of "trap doors" in sharable system routines at runtime. This method enabled us to steal control of all runs of users who called the system routines. At the user's expense, we were able to covertly copy his files. Had we wanted to, we could have destroyed or selectively rewritten them.

Section II - COMMON FAILINGS OF OPERATING SYSTEM DESIGN

(U) Operating systems are huge and complex sets of interacting programs. The current level of Exec VIII comprises about 500,000 lines of assembler code, and was written and modified by hundreds of programmers. We claim that no individual can understand such large and haphazardly constructed systems, and that such systems are bound to have holes. Emerging design techniques, such as "stepwise refinement" [6], "hierarchical design" [1,2], and "Parnas modularity" [3,4] are sorely needed methods of keeping large programs comprehensible. Until such design techniques are routinely used for OS developments, large OS's will continue to be highly insecure.

(U) Another characteristic impediment to the design of secure OS's is that many of the designers were trained on first and second generation systems, and their experience has resulted in an underestimation of the data security problem in a multi-programming environment.

(U) At the dawn of the computer age, most machines (e.g., Univac I, IBM 701, NAREC) did not have operating systems; instead, a group of commonly used subroutines was made available to each programmer to be used at his discretion. The programmer was not forced to use any of the common routines because he could write his own. This state of affairs was bearable because each programmer had the full use of the machine when his job ran. Thus, there was no need to think about protecting data in runs from other runs.

(U) Second generation computing (e.g., Univac 1107 under Exec II, IBM 7094 under IBSYS) was characterized by primitive operating systems whose functions were the scheduling of programmer runs and the service of I/O devices that runs used. Again only one run was executed at any time, but it was scheduled and serviced by the operating system and machine operators, thereby removing programmers from the computer room. Many second generation machines lacked memory protection, so that a programmer's error (for example, an array index out of bounds) could destroy the operating system, and force reloading of the backlog of runs waiting to be executed.

(U) Since in second generation systems only one run was executed at any time, the program protection problem consisted of preventing the operating system and the executing run from destroying each other. This problem was solved for the operating system by hardware protection of executive memory and "privileged" mode of operation which overrode all hardware protection of facilities. The user run, which operated in unprivileged mode, was unable to harm the OS; but since the OS had access to all machine facilities, it could, if not debugged, destroy user runs. However, this seldom resulted in the compromise of user data, since the executing run was the only run active when it was destroyed. Thus, the OS did not need to be foolproof in order to be of use; if it destroyed a run, the run was simply reloaded.

(U) Unfortunately, the same design and implementation practices that produced these early OS's were also applied to the problem of constructing MLS's with disastrous effect. The program protection problem is a fundamentally different one in a multi-programming environment. It is not acceptable for a MLS system to contain errors because more than one run will have access to the results of the system's mistakes. The highest priority in the design of an MLS system should be program security instead of throughput and ease of use, as was the case with more primitive systems.

Section III - SPECIFIC WEAKNESSES OF EXEC VIII

(U) The previous section described some of the design practices that result in programs that do not perform as specified. However, even if an MLS is completely bug-free, in the sense that its response to user requests is completely specified by its design, this does not imply that the MLS will not permit dissemination of data to unauthorized users. Our penetration of Exec VIII is not based on bugs in the implementation, though they certainly exist. Instead, we exploit several aspects of the Exec VIII design philosophy which, when taken together, make penetration possible. Some of these design features are listed below; the glossary in Appendix B defines the Exec VIII terms used.

(U) 1) Error Recovery. Error recovery in a multi-tasking environment is a source of breaches of security on many systems. In Exec VIII, any task may, via an executive request, cause error conditions produced by any other task belonging to the run to be captured in the requesting task. If any other task in the run posts an error-catching routine at some later time, this deletes the previous request, rather than stacking it. Thus, it is possible for a user's routine to catch errors generated by systems software. In general, when an error is fielded, the error-handling routine has access to everything that the routine causing the error has access to. Thus, if a task which calls a system routine can cause an error condition to occur in the system routine (such as a memory reference out-of-bounds error or even a divide overflow), the calling task could field the error with the resulting ability to reference programs and data within the address space of the system routine. The question of how to cause errors is resolved by setting up an improper environment for the routine to execute in, explained by the following.

(U) 2) Ill-Specified Program Environments. Let the totality of conditions under which a program runs be called the programs's environment. This includes register values, memory bounds values, names and contents of files assigned, etc. One of the most difficult problems in MLS design is that of making sure that the environment prepared for a system routine by a user's calling task is the correct one. In order to solve this problem, it is necessary to formalize the concept of an environment and specify environment-changing rules which are to be obeyed by user tasks which call systems routines. Such rules are not enforced under Exec VIII (or even, to my knowledge, stated as guidelines); this is partly due to the overhead required by enforcement, but is largely because the question of environment was a fuzzy one in the minds of the designers.

(U) Under Exec VIII, there are a number of ways to construct environments for system routines which cause errors; the easiest is to place the bank of core that the routine uses as a data area lower or higher than the system routine "expects" it to be, causing a guard mode (memory reference out-of-bounds) error.

(U) 3) Unprotected Reentrant Processors. The problems of error recovery and environment checking converge to disastrous results in the case of sharable systems routines which are not part of the operating system (e.g., compilers, editors, and data base management systems). By and large, operating systems protect themselves from bad environments and cause error returns which do not give the user's calling task greater access than before the call, but such care has not been taken, under Exec VIII at least, to protect sharable non-executive routines. Such routines are called Reentrant Processors

(REP's) on the 1108 because they are supposedly time-invariant (unmodifiable) program instructions and constants. A user requests the execution of a REP by means of an executive request, having previously prepared a core data area with the proper values. If an error occurs inside the REP, and the REP has not yet put in a request to handle its own errors, control will be returned to whichever task has requested to perform error handling. However, the task receiving control now has access to the REP, whereas before the link to the REP, it could not reference it.

(U) Once the user has access to the REP, the 1108 cannot prevent a user from altering the core memory allocated to the REP. The reason for this is a hardware design oversight. 1108 hardware provides for write protection of both the instruction and data banks, or for neither. Since REP's, which are instruction banks, must be able to alter their associated data banks, the REP's themselves must run unprotected. This failure of memory protection in the case of REP's has been documented by Univac [5].

Section IV - DETAILS OF THE SUBVERSION

(C) These design errors in Exec VIII provide the basis for our method of illegal penetration. The program written to take advantage of the opportunities to subvert REP's offered by Exec VIII is composed of two tasks: a BREAKER, which gains access to the victim REP, and a STEALER, which itself is a REP. Since we are interested in surreptitious entry, the highest priorities were to provide seemingly normal execution of the REP we were breaking and to structure the program so that no entries were written in the system log as a result of its execution. The function of the BREAKER is to prepare an out-of-bounds data bank for the victim REP and link to it, having previously requested to handle any resulting errors. The REP causes a guard mode error in trying to reference its data bank, and control returns to the BREAKER, but with access to the REP. The BREAKER changes the entry point instruction of the REP to a jump to the end of the REP, where, as a result of the Exec VIII core allocation policy, there usually remain a number of unused words at the end of the last core block allocated to the REP.

(C) The BREAKER then determines whether there are enough free words to enter a calling sequence to the STEALER and code to eradicate the visible effects of the call. If there is enough core, the BREAKER makes these changes; if not, it takes an error exit.

(C) Sooner or later, the REP will lose its core allocation, and since they are supposedly unalterable, REP's are not swapped out, but only in. So the BREAKER must reawaken periodically to see if the REP is still in core. If it is not, the BREAKER asks for it to be brought in again, and when it arrives, breaks it again. This cycle goes on until the machine goes down or the run is removed or a user links to the altered REP. The amount of processor time required to maintain the BREAKER is negligible; a run which kept the Univac assembler broken for about eight hours used thirteen seconds of processor time.

(C) When a user links to the broken REP, control passes through the calling sequence that the BREAKER added to the REP to our STEALER. It is evident that the STEALER must be a REP since many users may simultaneously link to the broken REP and end up in the STEALER. Also, the only easy way to make a routine accessible across run boundaries is to make it a REP.

(C) What the STEALER does when control from a user of the victim REP passes to it is immaterial; the penetration has already occurred. The STEALER has complete control of the user run and could:

1. Steal all assigned user files.
2. Destroy all assigned user files.
3. Selectively rewrite user files.
4. Terminate the user run.
5. Control any device assigned to the user.
6. Use all the machine time allocated to the user.

Since we are interested in covert entry, our STEALER merely steals assigned user files, writing them to one of our files. The STEALER then exists and control is returned to the victim REP with the user none the wiser.

Section V - LEVEL OF EFFORT REQUIRED

(C) This technique was suggested by Prof. M. Lay of the University of Maryland. A copy of his original memo describing the method, dated July 27, 1973, is contained in Appendix A. As is readily verified, our BREAKER operates exactly as prescribed in the memo and was running one month later. The STEALER is much more sophisticated than Prof. Lay described it because we wanted to avoid writing entries in the system log which would make the method discoverable after the fact. The problem of debugging the STEALER was greatly complicated by the fact that Exec VIII refuses to prepare core dumps of REP's. So, whereas the BREAKER took 2-3 man-weeks to develop, the STEALER required 3 man-months. However, it should be emphasized that once the BREAKER was running, the penetration had occurred. Our STEALER just provides some complicated bells and whistles which enable the victimized users' data to be stolen.

(U) When we began "production" runs, we were immediately faced with an information-pollution problem. We couldn't possibly manually look through all the files that we stole, so we developed a set of service routines to bring the stolen information into tractable form. One service routine reconstructed files so that we could examine them with Univac's editors and file utility routines. We were able to execute the programs contained in the stolen files. We found that the file space required to store the stolen data was as large as one tenth of the total mass storage available on the 1108 system, and were forced again and again to restrict the class of users from whom the program would steal. At the end of the effort we only accepted data from classified users running in batch mode.

Section VI - HOW CAN THIS HOLE BE FIXED?

(U) The obvious fix is to change the 1108 hardware so that write protection is available for I-banks without requiring it for D-banks. Such a hardware change is available for less than $1000 from Univac. Installation of this change would require modification to systems programs. Any one of the following software changes should also fix the problem; they are ranked in increasing order of estimated man-hours required:

(U) 1) Change every REP so that it clears all error-handling facilities by means of a special trick: if the REP submits an erroneous error-handling request, the system responds by deleting the previous error-handling facilities and not entering the new erroneous ones. Thus, the REP may, by dint of this special case, remove all error handling set up by a calling program. It is then free to set up its own contingency routine. One REP on the University of Maryland's Exec VIII system is known to operate this way; this is probably the easiest method of software protection.

(U) 2) Change the REP calling sequence internal to Exec VIII so that no routine other than the REP may field errors generated by the REP. This seems easy, but has extensive ramifications. For example, a user may want to create a REP which will characteristically perform an error return, and whose result is specified by the type of error generated. The author is aware of several programs that operate in this manner. Another ramification of this method is that it restricts REP to REP linking, since even REP's would not be able to catch errors generated by REP's that they call.

(U) 3) Change every REP so that it checks for the possibility of being called in an erroneous environment. This is very costly, since every REP must be modified and modification of each REP requires an understanding of the contingencies that particular REP could encounter.

REFERENCES
(Unclassified)

[1] Dahl, O., and Hoare, C. Hierarchical Program Structures, Structured Programming, Academic Press, New York, N. Y., 1972, pp 175-220.

[2] Dijkstra, E. W. The structure of "THE" - multiprogramming system. Comm. ACDM 11, 5 (May 1968), 341-346.

[3] Parnas, D. L. A technique for software module specification with examples. Comm. ACM 15,5 (May 1972), 330-336.

[4] Parnas, D. L. On the criteria to be used in decomposing systems into modules. Comm ACM 15, 12 (December 1972), 1053-1058.

[5] Univac 1100 Series Systems, USE-UUA/E Conference Notes. Univac USE Conference, Spring, 1974, New Orleans, La., p. 4-38.

[6] Wirth, N. Program development by stepwise refinement. Comm. ACM 14, 4 (April 1971), 221-227.

ACKNOWLEDGEMENTS

(U) I would like to thank Dr. Micheal Lay of the University of Maryland for the aid and direction he supplied during the design and debugging of the programs that performed penetration of the Univac 1108 Exec VIII system. Indeed, he supplied the original scheme of penetration.

(U) I am also indebted to Dr. John Shore and Mr. Stanley Wilson of the Naval Research Laboratory for their highly constructive review of the early drafts of this Memorandum Report.

APPENDIX A

ORIGINAL PROPOSAL FOR SUBVERSION

Exec 8 Subversion: Reentrant Processors (REPs) - General

(C) The implementation of reentrant processors under Exec-8 may yield a gateway to the subversion of runs concurrently sharing a procedure portion of a REP. The REP philosophy is fundamental and could yield:

a) names and access keys to files attached to other runs

b) access to files assigned to other runs

c) read access to any part of the Exec

Reentrant Processes

(C) The reentrant process is a pure procedure shared by many users of the system. As implemented under Exec-8, the REP is created with an I-bank only. It is assumed that no instructions modify any portion of the I-bank.

(C) To use a REP, an initialization process is constructed entirely within the D-bank. When the REP I-bank is needed, a LINK to the REP entry point is executed. The Exec has been informed of all REP entries and, through a series of tables, links the REP I-bank to the user's D-bank and transfers control to the REP procedure. The REP, now supplied with a D-bank, performs its normal function.

Subversion Technique

(C) The key to subverting the REP lies in modifying the I-bank of the REP so that when another run is dispatched which uses the REP, subverting activities can be performed in that user's environment. Thus, the following steps must be taken:

a) force processor control to the D-bank after the link to the REP has occurred.

b) modify the REP I-bank to perform the activities desired.

c) continue to perform modifications for the duration of the run.

(C) The addressing scheme of the 1108 aids in the completion of part a). All data references are modified by the base-relocation hardware registers of the CPU. The program counter, however, is always maintained in absolute (any loading of the PC is done after relocation). Thus, if the first relocatable address of the D-bank is greater than can be held in the operand address portion of an instruction (16 bits), the REP will cause an address exception with any reference to the D-bank. (Note, the program within the D-bank must always make data references by indexing to create a full 18 bit address. Execution is possible in the D-bank since the PC is absolute). Therefore, the D-bank program must:

1) Register a guard mode contingency with the Exec

2) Link to the REP

3) Catch guard mode - REP is in I-bank

4) Modify REP

5) Handle results

Modification suggestions

(C) Probably the simplest action which would cause little disturbance is to copy all files attached to the user's run by causing his run to copy the files to the public domain. This can easily be accomplished by:

a) reading the user's PCT and noting all assigned files

b) creating a file containing Exec-8 control cards to copy these files

c) adding this file to the user's runstream through CSF$

(C) At some later time, at the leisure of the subverter, the files may be examined, copied to tape, etc.

W. Michael Lay
July 27, 1973

APPENDIX B

GLOSSARY (U)

Bank:	An area of core which is some integral multiple of 512 words in length. Programs on the 1108 normally have two banks: an instruction bank and a data bank.
Contingency:	An error condition generated by execution of a program which intercepts the program and causes control to be passed to a user- or system-provided routine which takes care of the consequences of the error.
Data bank or D-bank:	A bank which normally contains data or instructions which may be modified in the course of program execution.
Error handling routine:	A user's task which is activated when a contingency occurs during exeuction.
Error condition:	Synonymous with contingency.
Error recovery:	The process of recognizing and responding to a contingency.
Executive request:	An instruction which causes an interrupt to Exec VIII from a user's program. This is the way that users communicate with and request services from the executive.
Guard mode:	This is the contingency that occurs when a system or user program attempts to access a core location which is not contained in the I-bank or D-bank of the program.
Instruction bank or I-bank:	A bank which normally contains program instructions and constants.
Link:	This verb is used to denote the process that occurs when a user program issues an executive request to enter a reentrant processor.

Reentrant Processor or REP:	An instruction bank is a bank which theoretically is not modified during normal execution, and therefore may be shared by a number of users. Execution of a REP is initiated by a user request to link to it, which attaches a user data bank to it.
Run:	Synonymous with job. A sequence of program executions, requested of the executive system by job control language statements. Each program executed may activate a number of tasks.
Task:	Though Univac uses the term <u>task</u> for another purpose, we will define it as a virtual CPU which performs one phase of the execution of a program. A task may create new tasks, or deactivate old ones. All tasks involved in the execution of a program share the I-bank and D-bank created for the program.

JANUARY 14, 1977.

MEMORANDUM

To: Senator Ribicoff.
From: Fred Asselin and Philip R. Manuel.
Subject: ADP Security in Unclassified defense Matters.

The staff study, "Computer Security in Federal Programs," will be enhanced by the inclusion of a paper prepared by William S. Franklin, Computer Systems Analyst, Directorate for Automation Policy, Technology and Standards, Office of the Secretary of Defense (Comptroller). The article is entitled, "DOD Interest in ADP Security For Unclassified Arena."

DOD INTEREST IN ADP SECURITY FOR UNCLASSIFIED ARENA

Although current DOD ADP policies concentrate on the protection of information essential to National Security, there is a continuing interest in the protection of that information which is unclassified. This interest in the unclassified arena has become more intensified by the passage of "The Privacy Act of 1974" (Public Law 93-579) and three recent GAO reports on computer security (i.e., "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities," "Improvements Needed in Managing Automated Decisionmaking by Computers throughout the Federal Government," and "Computer Related Crimes in Federal Programs"). With the above events, computer security with respect to unclassified information has become more than a matter of concern to DP and Middle Managers but more important a prime concern of top management.

Top management within the DOD have been aware of and concerned about the protection of classified information for quire some time. Moreover, their concern carried over to the protection of this type of information when processed by computer systems. This top level concern is currently reflected in DOD policy issuances such as DOD Directive 5200.28, "Security Requirements for ADP Systems," dated December 18, 1972 and DOD Manual 5200.28, "ADP Security Manual," dated January 1973. These policies call for a high degree of discipline in the establishment of a security posture. Emphasis is placed on areas such as risk analysis and planning, individual accountability, environmental control, data integrity and the like. We all recognize these as necessary conditions for data security.

Many middle managers within the DOD have applied the concepts of the above policy issuances to the protection of unclassified information. Their major concern being the protection of data systems from possible fraud, embezzlement or natural disaster. However, this has not been done on a uniform or consistent basis. Procedures for the protection of unclassified data systems while currently being developed within DOD, are very rudimentary at this point. Therefore, implementation of the policy espoused in DOD Directive 5200.28 and DOD Manual 5200.28M as applied to the protection of unclassified information has for the most part been neither formal, disciplined nor rigorous. However, with the increasing interest of top management, these shortcomings can be alleviated.

Increasing top level concern within the DOD is becoming more visible by the degree of interagency involvement of DOD personnel in data security related activities. For example, DOD participated on (1) Tasks Group 8 of the Domestic Council Committee on the Individual's Right to Personal Privacy; and (2) various Task Groups of the National Bureau of Standards concerned with data security. Outputs from these efforts include FIPS PUB 31 "Guidelines for Automatic Data Processing Physical Security and Risk Management," and FIPS PUB 41 "Computer Security Guidelines for Implementing the Privacy Act of 1974." Another event that indicates top level concern within the DOD is the current effort to establish a management staff within the Office of the Secretary of Defense to oversee and coordinate data systems security activities within the DOD. Specifically, this staff would:

1. Develop and provide technical advice and guidance with respect to DOD ADP security policy.
2. Effect coordination and interchange of information on ADP Security technology within DOD and between the DOD, other government agencies and private industry.
3. Design and promote programs identified to meet common functional needs.
4. Prepare appropriate ADP security technological program assessments and plans.
5. Assist in evaluating the ADP security programs of the DOD Components and advise the OSD Program and Budget Office on their adequacy.
6. Coordinate with the DOD Components to ensure the availability of technical support.
7. Issue guidance and direction to ensure the timely development and implementation of ADP security safeguards to support compliance with the Privacy Act of 1974.

The preceding initiative at the OSD level is merely one aspect of DOD Automation Objective #6, "Safeguard Personal Privacy and Improve ADP Security." A related and necessary initiative on the part of top management is the development of an ADP system life cycle management policy which emphasizes among other things ADP security. The ADP system master plan that will be required by this policy can serve as the basis for instituting formalism and discipline into the protection of unclassified information.

The preceding initiatives coupled with related concerns such as Privacy will give continuous impetus to the area of data security. As alluded to above, with the increasing concern of top management ADP security as a formal discipline will become a reality in the DOD.

○

END