

*Memorandum*

January 4, 1979

CG-79-12

TO : Heads of Divisions and Offices

FROM : Comptroller General

*Frederic A. Steeds*SUBJECT: Briefing on Automatic Data  
Processing, February 13

There have been a number of recent articles and speeches on what may be loosely called a revolution in the field of data processing and computer technology which is not only altering the cost of data processing but also the application and controls associated with data processing equipment. The attached special report which was contained in the July 1978 issue of Dun's Review is an example, but similar articles have appeared in Fortune, Business Week, and elsewhere.

Because data processing is changing so rapidly, I have asked Don Scantlebury to arrange for a briefing on the expanding power, potential, and problems of ADP to give us an opportunity to learn more about these developments, particularly as these trends impact on government, business, and society. These developments can also have a major bearing upon GAO's work. The tentative assignment lists of FGMS, also attached, for September, October, and November, reflect to some extent these newer developments and I would hope we could, in our discussion, focus on this listing as well as other work which we have in process or in our future work plans.

The all-day briefing session will be in Room 7315, on Tuesday, February 13, 1979. Please mark your calendar and reserve that date. A more detailed program for the day will be sent to you by mid-January. I suggest that you also arrange to have present your ADP liaison, your deputy, and anyone else whom you think would have a particular interest or responsibility in this area.

We would also like to address ourselves to any questions you may have on this subject. Please forward questions you would like to have answered during the briefing to Mr. Walter Anderson in FGMSD-ADP by January 19, 1979. The program format will also permit time for other questions to be discussed as they arise.

Mr. George Sotos (Ext. 55040) can provide you any additional information desired.

Attachments

DISTRIBUTION: Code B

GAO BRIEFING ON AUTOMATIC DATA PROCESSING

FEBRUARY 13, 1979

THE CHANGING WORLD OF THE COMPUTER

<u>Time</u>	<u>Subject</u>	<u>Speaker</u>
8:30	Welcome and Prefatory Remarks	Mr. Elmer Staats Comptroller General
8:40	Introduction and Overview	Mr. Don Scantlebury Director, FGMSD
8:45	Briefing Format and Expectations Review Agenda Identify "Selected Articles", Displays, Demonstrations Introduce Film	Mr. Walter Anderson Associate Director, FGMSD
8:55	"At the Forefront"	Film
9:30	The ADP Marketplace	Mr. Walter Anderson
10:15	Automatic Data Processing Futures: A Consultant's View	Mr. Ted Withington Arthur D. Little, Inc. (on video)
10:30	Break: Coffee Served View Displays and Demonstrations	Attendees
10:50	The Industry Viewpoint	Mr. Jack Jones Vice President Southern Railroad
11:50	View Displays and Demonstrations	Attendees
12:15	Lunch in Dining Room	Division/Office Heads Guests
1:15	Transnational Data Flow	Mr. Blake Greenlee Assistant Vice President Citibank
2:15	Privacy and Security	Mr. Bob McKenzie Audit Manager
3:00	Break	

IMPLICATIONS OF ADP FOR THE GAO

<u>Time</u>	<u>Subject</u>	<u>Speaker</u>
3:15	Presidential Reorganization Committee Report	Mr. Pete Jensen Georgia Institute of Technology
4:15	Implications for GAO Audit Work	Mr. Don Scantlebury Mr. Mike Zimmerman, Assistant Director, HRD
5:00	Briefing Close	Mr. Staats Mr. Scantlebury

We hereby express our appreciation to the following units for the supportive cooperation and excellent services they provided in the preparation for and implementation of the briefing and for the production of related materials:

- All speakers (identified on the next page) for their briefing presentations.
- FGMS Division (ADP Group) facilitators (identified on the next page) for providing assistance and support to the Program.
- GAO divisions for designing the displays and preparing the demonstration.
- Illustrating Services for the numerous graphics (see section 13) produced for the displays, the demonstration, and the "Selected ADP/Auditing Articles" and "Briefing Summary" publications.
- Printing Services for printing the "Selected Articles" and "Briefing Summary" publications.
- Audio/Visual Services for producing the audio tapes from which the speaker sections of this Summary are reproduced.
- FGMS Division editors for editing the briefing presentations.
- FGMS Division secretarial staff for the typing work.
- Information Officer for reviewing this Summary.
- UNIVAC, IBM, and Hewlett Packard for providing the film, slides, equipment pictures, and computer components for the current technology exhibits.
- FGMS Division ADP Education Program staff for managing the development and coordination of the "Selected ADP/Auditing Articles" material.

GAO OFFICIALS AND SPEAKERS



ELMER STAATS  
CG



DONALD SCANTLEBURY  
FGMSD



WALTER ANDERSON  
FGMSD



DONALD EIRICH  
LCD

GUEST SPEAKERS



TED WITHINGTON  
ARTHUR D. LITTLE INC.



JACK JONES  
SOUTHERN RAILWAY



BLAKE GREENLEE  
CITIBANK



PETE JENSEN  
GA. INST. OF TECH.

GAO SPEAKERS



ROBERT MCKENZIE  
LCD



MIKE ZIMMERMAN  
HRD

GAO FACILITATORS



KEN POLLOCK  
FGMSD



GEORGE SOTOS  
FGMSD



CHARLES SHIMKUS  
FGMSD  
Program Coordinator



DAVE DORE  
FGMSD

IMPLICATIONS OF CHANGING  
COMPUTER TECHNOLOGY FOR GAO

by

Elmer B. Staats  
Comptroller General  
of the United States

February 13, 1979

Mr. Staats

Let me start by saying that I think this is a most important meeting for GAO. We all have many problems to deal with in our day-to-day work, and we certainly don't look for new ones, but the computer--and all it has done to revolutionize information technology--is with us to stay. It is constantly enlarging the scope of its presence, and its impact on Government operations is increasing daily.

Today you will be hearing about some of the recent technological advances in ADP and telecommunications, and the effects they are having on management of organizations from the largest to the very smallest. The rate of these advances is quite remarkable, and is one of the few bright spots in improving national productivity. The computer industry is also one of the few bright spots in dealing with our balance of trade problems. For example:

- ° In medicine, computer tomography scanners are permitting 3-D analysis of the organs of the body, aiding in accurate diagnosis of some problems which up till now could be diagnosed only through more painful methods such as exploratory surgery.
- ° Electronic message service cost is already comparable to that of first-class mail, and it is going to have a marked impact on the operations of the Postal Service.
- ° In the financial area, it is unbelievable how much money is already flowing through electronic funds transfer systems daily. On FEDWIRE alone, developed by the Federal Reserve Board, over \$43 trillion was handled in 1977, and the volume is growing. Banking will never be the same again.
- ° The Control Data Corporation has recently announced a new model--the CYBER 203--which can process over 100 million instructions per second. It has been estimated that applying a machine of this power will improve weather forecasting to the point of avoiding over \$1 billion annually in weather-related losses in this country.
- ° Small business computers are virtually flooding the country.

- ° Microprocessors are already used in some automobile models.

As these developments occur, they bring into sharp focus many of the problems Government has been wrestling with for years. For example, the availability of relatively low cost minicomputers and microprocessors--many with the capabilities of large computers of just a few years ago--suggests the need to review agency postures on decentralization. At the same time, new microwave communications capabilities for computers permit linking of computers at great distances, and this presents opportunities for timely centralized control of widespread activities to a far greater extent than before. The potential for improved Government operations generally is great, but this positive potential is matched by a negative potential of disrupting ongoing operations if the transition to such changes is not carefully and competently managed.

Just a couple of weeks ago, after President Carter created the Federal Regulatory Council, it was recognized that a crucial cog in the plan to coordinate regulation was development of a data base that can be used to analyze the impact of current and proposed regulations. If this data base is properly designed and maintained, it will present important opportunities to improve this area of government operations. On the other hand, a poorly designed system may well result in complete frustration of efforts to do a better job. It is this reliance on the computers, their communications, the accuracy of the data, and the systems design that mandate serious management involvement and control. Obviously, if agency management needs to be knowledgeable, we need to be also.

I consider it essential for GAO staff, particularly at management levels, to be sufficiently knowledgeable in the subject of computers that we can do a good job in assessing this rapidly evolving role of the computer in the operation of the Government. Similarly, we need to have excellent staff level capability to evaluate the adequacy of computer controls, effectiveness of computer applications, and efficiency and effectiveness of the systems development process in the agencies.

We are going to have to move with the times and make sure our audit approaches take into account both the situation as it exists today and the dynamics of change. You should consider this in light of your assigned responsibilities, and take whatever additional steps are needed to assure yourself that you have this area under control.

There have been a number of dramatic computer-related fiascos--Secretary Califano's apology to the American Medical

Association for using inaccurate computer-generated information to publicly criticize physicians' activities in Federally funded medical programs comes to mind. We must avoid any such embarrassments for the GAO.

Today, we can no longer get by with stating the information in our reports "was taken from the agency's automated records"; we have a duty to verify its accuracy and reliability. This means that we must live up to our own standards of auditing when we are dealing with computer-based agency systems.

The recent HEW conference on Fraud, Abuse, and Error highlighted many difficulties with computerized systems. The \$10.2 million theft from Security Pacific Bank is just another example. How many of you know that the bank was not aware of its loss 8 days after the act was perpetrated? And that they learned of it then only because the FBI, in tracing the diamond transaction, called them to try to check on the source of the money? Again, our friends in the FBI had been telling us that another Equity-Funding type scandal was about to hit the newspaper, and it broke in the January 22, 1979, Computerworld issue--a multimillion-dollar computer fraud in the insurance industry in Texas.

If situations of this type can occur in what we would expect to be well-controlled operations, it does make one wonder just how bad things might be in Government. This is particularly true when we consider the reports we have issued indicating frequent existence of very weak controls in Government ADP systems. Our work on computer security, computer crimes, automated decisionmaking systems, and other assignments does cause one to wonder--"What is going to happen next?"

As Comptroller General, I have no desire to appear before the Congress to make excuses for missing, in our work, major deficiencies in agency computer operations.

I do feel that our ADP audit capabilities have been significantly improved in recent years, but--as you will learn today--this is no time to rest on our accomplishments. Again, the rate of change is accelerating and we must move with it.

In recognition of this change, Don Scantlebury has just completed work on revisions to our yellow book specifically setting forth supplemental audit standards in dealing with computer systems, and I'm sure you will be interested in what he has to say about them and their effect on our work.

In a related area, we are receiving congressional requests for evaluations of the quality of ADP management in Federal

agencies. In view of the billion of dollars expended annually by the Federal Government through computers, and our responsibilities concerning these Federal expenditures, I think we can anticipate many more such requests in the future. The Presidential Reorganization Project (PRP) on ADP is nearing completion. Pete Jensen, who has been a real driving force in the project, will be talking to you later today. I don't want to steal Pete's thunder, but listen to one of their major findings:

"The Federal Government is, in general, mismanaging its information technology resources and has not developed a plan for exploiting the opportunities of the future with respect to investment, service delivery protection of citizens, or national security."

One of the causes of this situation is reported by the PRP group to be:

"Abdication by Program agency management of its responsibility for managing information technology as a mission-oriented resource."

We in GAO have been hammering away at poor management of ADP systems, but I am not satisfied that we have done enough, and I am concerned for tomorrow.

We want to make ADP audit work an attractive career in GAO, so that we will have the capability to perform up to expectations. Our audit work in each agency must deal with the computer in an exemplary manner or we will be subject to scathing and justifiable criticism. We have already taken the agency internal audit groups to task for aversion to computer work, but--even if they make an excellent response--we can't rely on them to do it all.

I hope we will have a "no-holds-barred" discussion on this matter at the conclusion of today's formal presentations.

INTRODUCTION AND OVERVIEW

by

Donald L. Scantlebury  
Director  
Financial and General Management Studies Division  
U.S. General Accounting Office

February 13, 1979

HARDWARE, SOFTWARE,  
INDUSTRY STATISTICS, AND  
DEPENDENCY ON COMPUTERS

by

Walter L. Anderson  
Senior Associate Director, ADP  
Financial and General Management Studies Division  
U.S. General Accounting Office

February 13, 1979

## Walter Anderson - Summarized

### Part 1. Computer Hardware

At the beginning of the day's activities, the motion picture "At the Forefront" showed a brief history of computers. The film ended with several scenes showing present-day computers and the process of producing the microscopic-sized components. My remarks will pick up from there and, with the help of some slides, I will show why computer equipment, or hardware, costs are going down and why the programing, or software, costs are not.

The slides of computer logic circuits show four generations. First, vacuum tubes were used with electrical components. They were assembled by hand-labor and wire connections were soldered individually. Later, transistor circuits consisted of parts inserted in holes in a circuit board with copper strips serving as wires. These were prefabricated by an etching process. Soldering was done by exposing one side of the board to another solder bath.

In further progress toward automatic fabrication, both wires and components were deposited or etched out to make complete circuits. Current technology permits the automatic fabrication of thousands of circuits on a small "chip" of semiconductor material.

Computer memory circuits for the "main" memory storage function were, for many years, made of little magnetic doughnuts, or "cores." Each core can store one element or "bit" of information (yes or no, on or off). Combinations of these elements are used to identify decimal digits, alphabetic letters, or special symbols. Arrays of these cores had to be assembled by hand with three wires threaded through each core. This process was never fully automated. Over the years memory elements have been developed that can be manufactured by automatic processes such as photo-engraving and etching.

Computer logic circuits and memory circuits can now be manufactured together on the same chip. And, these chips can be manufactured automatically dozens at a time. A typical example is a microprocessor, or personal computer, such as Zilog Z80. The Z80 contains 8500 transistors in logic circuits plus main memory storage in a chip the size of the head of a paper match. It requires only a keyboard, a numeric display, and a power supply (battery) to be a functioning computer.

Clearly, automatic mass production in place of hand-assembly and soldering, has been the key factor in reducing the cost of computer components. The attached excerpts from the February 5, 1979, issue of Computerworld illustrate the dramatic reductions

in terms of IBM equipment. Other manufacturers, of course, must be competitive as IBM price reductions are typical of industry trends.

## Part 2. Industry Statistics

Walter Anderson reviewed the computer industry by presenting colored slides taken from the International Data Corporation presentation published in Fortune Magazine, June 5, 1978. The slides have been reproduced in the publication, Selected Articles on ADP Auditing, for the Executive ADP Briefing, February 13, 1979, pages 211-222.

The slides showed the relative sales of IBM and the six billion-dollar dwarfs:

- Sperry Univac
- Honeywell
- Burroughs
- NCR
- Control Data
- Digital Equipment Corporation

Other slides included:

Computer spending in large organizations in the U.S.

The international and domestic markets for general purpose computers built by U.S. manufacturers.

The small business computer marketplace.

The mini-computer marketplace.

Computer-related bank, fraud, and embezzlement.

The growth of general purpose computers built by U.S. companies.

The computer services and software market.

## Part 3. Software

In our previous remarks, we noted how computer hardware prices have been reduced over the years because the construction process has been automated. Software, on the other hand, continues to be done by hand without the benefit of much in the way of tools or automatic production machinery. It is true that the computer programming languages that are called "high level" do permit programmers to use fewer instructions than the previous

The most controversial part is conversion.

Conversion is the change from one computer to another. What makes it controversial is that the substantial expense of conversion leads organizations to keep the same brand of computer rather than procure by competitive bids. Two congressional committees, Government Operations and Appropriations, have taken almost opposing views on whether or not conversion expense is a cost factor to be considered in evaluating proposals and offers.

The most undeveloped part is software standards.

There is only one Federal standard language, COBOL. While there are other commercial standards, the Government has lagged behind in both standards, development, acceptance, and compliance.

The forgotten part of software is auditability.

Computer programs are seldom designed with the auditor in mind. We advocate auditor participation during the development process to assure that software can be audited.

By this method of presentation, we have shown some of the difficulties with software, so we are now ready to answer the question, "What is the hardest part of the software?"

If you haven't guessed it by now, the hardest part is management control. Considering the above problems, management has a real challenge in trying to control the software process and the personnel involved. Our ADP issue area work is dedicated heavily toward improving the entire area of software management control.

#### Part 4. Dependence on Computers

To complete my presentation, I will point out the heavy dependence we have on computers. This is important to us in GAO in trying to assure that Federal systems will function without unwanted interruptions.

A few years ago a nationwide survey was conducted by Time Magazine and the American Federation of Information Processing Societies. Here are two of the questions and answers.

"Do you currently have a job which requires some contact with a computer--either directly or indirectly?"

30 percent said, "Yes."

"Does your job require that you have some knowledge of how a computer system works?"

85 percent said, "No." But,  
15 percent said, "Yes."

From our own experience in analyzing the ADP operations of a major Federal agency, we found that the computer hardware classified as assets on the balance sheet amounted to about 5 percent of total assets. Annual expenses for computer operations, including personnel, were in the range of 15 to 20 percent of total expenses. But the dependency of the agency on computers appeared to us to be about 100 percent. They could not operate long without their administrative and scientific computers.

Now, in many areas dependence can lead to serious problems. For example:

At a hearing of the Electronic Funds Transfer Commission, Computer Crime Investigator, Donn Parker was asked, "What is the likelihood of a multimillion dollar electronic fund transfers crime involving Federal funds in the following year?" He answered that it was very likely.

Here is a hypothetical example proposed by Dan MacCracken, President of the Association for Computing Machinery. A series of major air crashes taking lives of hundreds of people is traced to sloppy programing!

We, at GAO, have much to do in ADP because of the increasing dependence on computers.

Table 1

IBM SYSTEM	370/115-0	370/125-2	4331	370/138	370/148	4341	370/158-3	3031
<b>CHARACTERISTICS</b>								
Relative Performance <sup>1</sup>	2.25	6.3	11 <sup>**</sup>	11.7	24	37 <sup>**</sup>	45	54
Memory Size in Bytes (Minimum to Maximum)	65K-384K	96K-512K	512K-1M	512K-1M	1M-2M	2M-4M	512K-6M	2M-6M
Purchase Price <sup>2</sup> (Memory Size)	\$91,000 <sup>*</sup> (384K)	\$179,750 <sup>*</sup> (512K)	\$68,760 <sup>*</sup> (512K)	\$271,260 <sup>*</sup> (1M)	\$450,300 <sup>*</sup> (1 M)	\$248,760 <sup>*</sup> (2M)	\$1,545,365 (2M)	\$1,000,000 (2M)
Monthly Lease (Lease Term)	\$2,850 (4 Years)	\$5,915 (4 Years)	\$1,879 <sup>*</sup> (2 Years)	\$10,439 (4 Years)	\$17,624 (4 Years)	\$6,069 <sup>*</sup> (2 Years)	\$44,255 (4 Years)	\$25,000 (4 Years)
Memory Cycle Time (Nsec)	480	320-480	1,300 (Per 4 Bytes)	715-935	405-540	Not Available	650-1,035	345
Machine Cycle Time (Nsec)	480	480	900 (Per 4 Bytes)	275-1,430	180-225	150-300	115	115
Channels (Minimum to Maximum)	1	1	0-2	3	5	3-6	0-6	6
Price per 1M Byte Of Main Memory	\$75,000 <sup>*</sup>	\$75,000 <sup>*</sup>	\$15,000	\$75,000 <sup>*</sup>	\$75,000 <sup>*</sup>	\$15,000	\$75,000	\$75,000

1. Relative throughput based on the IBM 370/158-3 equalling 45. Performance is based on IBM's claims at time of product announcement, later adjusted as user benchmarks and experience were reported. Compiled by International Data Corp.'s Information Systems Planning Service in cooperation with Computerworld. Performance figures for systems with an asterisk (\*) are based solely on the manufacturer's claims.  
 2. For a configuration including CPU, stated main memory, power supply, console and mini-

num channels.  
 3. Purchase and lease prices for the 4331 and 4341 include price of the 3278 Model 2A display console (purchase, \$3,760; lease, \$94) to conform to above configuration.  
 4. Purchase prices for 370/115, 125, 138 and 148 reflect newly reduced prices as of last week.  
 5. Price reductions on the above 370 systems affect processor and associated minimum memory. Price per 1M byte of memory increment is unchanged.

CW Chart by M. Rosenber

Table 1 shows two newly announced IBM computer systems in comparison to the present 370 Series Models. I want to draw attention to the Model 4341 and compare it to the 370-158-3. They are relatively close in relative performance, 37 units compared to 45 units. The new 4341 has a purchase price about one-sixth of the older model (1/4 million dollars compared to 1-1/2 million dollars) and the price to add main memory is one-fifth of the price for the older model. (\$15,000 versus \$75,000 per million characters, or "bytes.")

Table 2

IBM TECHNOLOGY INSERTION STRATEGY					
DISK			MEMORY		
Model	Year Announced	Bytes/\$1	Model	Year Announced	Price per 1M Byte
2311	1964	300	360/30	1964	\$2,000,000
2314	1965	1,300	370/155	1970	600,000
3330-SD	1970	3,800	370/135	1971	640,000
3340	1973	3,500	370/115	1973	300,000
3330-DD	1973	5,300	5100	1975	180,000
3344	1975	11,300	158/168	5/76	170,000
3350	1975	12,825	Series/1	11/76	120,000
3370	1979	16,268	3033	4/77	110,000
			8100	10/78	18,000
			30 Series	12/78	75,000
			4300	1/79	15,000

Chart courtesy of International Data Corp. Updated by CW for the 3370 and 3377.  
**The Declining Prices of Disk Storage and Main Memory From 1964 to the Present**

Table 2 shows the dramatic reductions in disk memory and main memory prices over the years beginning in 1964. As I said before, this reduction has come about by the automation of the production process. Note that the effects of inflation have been completely overwhelmed and are invisible in the dollar figures listed.

AUTOMATIC DATA PROCESSING FUTURES:

A CONSULTANT'S VIEW

A conversation between

Frederick G. Withington  
Arthur D. Little, Inc.

and

Donald L. Scantlebury  
Director  
Financial and General Management Studies Division  
U.S. General Accounting Office

February 13, 1979

## Introduction of Ted Withington by Walter Anderson

You are about to see a video-taped conversation between Don Scantlebury and Frederick G. Withington; called Ted Withington by most people. Ted is a graduate of Williams College with a B.A. in physics. He was associated with the National Security Agency as a computer programmer and programming supervisor. He later went into industry with Burroughs Corporation and was concerned with applications and installation of computer systems and participated in and directed many technical support programs. He has been at Arthur D. Little, Inc., since 1960. A. D. Little, of course, is a well-known consulting corporation. Mr. Withington has worked with virtually all aspects of the data processing systems, their designs, applications, markets, and interactions with the organizations using them. In the course of all this consulting work, he has become an expert in forecasting the future in ADP. He has also written four books. He is a regular contributor to the periodicals in our field. His annual articles in DATAMATION magazine on the future are landmarks. In the November 15, 1978, Special Issue on the Data Processing Industry in Transition, Ted Withington had the lead article. A copy of this article, "Transformation of the Information Industries" appears in the collection of "Selected Articles on ADP Auditing" which Chuck Shimkus prepared for this briefing.

We had the pleasure of working with Ted some years ago in the task group that helped us with management guidelines on cost control and cost accounting for computer-based information systems.

We call Ted the "expert's expert."

Don Scantlebury  
Ted Withington

Don: Ted, I'm sorry that your foreign trip is keeping you from live participation in the Comptroller General's February 13th program on ADP. But I'm glad we have this opportunity to go over some questions and answers for us to present to the group. As you are aware, the theme of the program for which this interview will be played is "The Changing World of the Computer--and Its Implications for the General Accounting Office." The questions we are about to ask you are in these two veins. First, let's concentrate on the current technological happenings.

What are some of the technological advances in computer hardware and applications likely to take place over the next few years?

Ted: I think briefly, there are three: First, there will be continuing reductions in the cost of semiconductor electronics to incredibly low levels. Second, there will be slow improvements in software to make the machines more automatic and therefore, somewhat easier to use. They will be more inefficient as a result, but many people will prefer that, I think. Third, there will be an ability to interconnect computers and many kinds of terminal equipments quite readily into communication networks.

Don: We have heard and read about these great technological advances--improved communications, networking, data base management and so on--but in the final analysis, what does this all mean for top-level general managers and how will it impact middle managers?

Ted: Well, of course, most management responsibilities will be unchanged, but there will be some options in style available. For example, with such systems a top manager would be able to participate directly in the on-going activities of his organization as they take place, if this is felt to be desirable. Contrary-wise, he could delegate authority to agents in the field on the basis that they have all the relevant information available to them. As for the middle manager, he could get badly squeezed under either scenario and his interest and his importance to the organization should be carefully considered.

Don: What are the most common mistakes you see made in the use of computers?

Ted: Probably short range thinking sums it up. The acquisition of equipment or the undertaking of a programming project with the idea of meeting just the immediate needs at a minimum cost, regardless of the long-term life cycle cost of it and of eventual transportability to some other computer look alike.

Don: Based on your experience, what effect do you think that the growing availability of smaller, cheaper, more powerful computers, and automated computer links will have on the organizational structure of major governments?

Ted: They will certainly permit further physical dispersal of the departments than has taken place so far, and as I just noted, they will permit a wider variety of changes in management styles than has been possible so far, either toward recentralization or decentralization of authority.

Don: How do you think these effects can be controlled?

Ted: Well, the effects of such systems on the organizations using them are typically very difficult to predict with any precision. So what people typically do is run carefully developed prototype experiments with careful management participation and oversight and then only after management is satisfied that in every respect this will be an improvement, should they authorize the general adoption of the new system.

Don: Because of high conversion costs, installations are locked into one manufacturer. How do you view this?

Ted: It is a very serious and general problem for large computer users everywhere. The future computer systems are likely to be able to run several kinds of software; that is the new and also the old, within the same complex of equipment and this will help, but in fact that probably will turn out for most users to be only a postponement of an inevitable day of final conversion of the old software.

Don: Most auditors are concerned with verifying information, and to do this they determine whether they can rely on systems to produce accurate results. This means they must study and evaluate the systems. But in GAO, we have the additional responsibilities of evaluating efficiency, effectiveness, and economy of program results. What methods and techniques can be used or are needed to address points in major complex systems?

Ted: Of course, I'm not an auditor, so I mustn't go too far with this, but I think there is one point in particular that I would recommend that is not very often done--called briefly a post audit. Most projects are undertaken with certain benefits claimed. The idea is simply to go back and see if the benefits were achieved. Along with this, all those benefits that the user department is responsible for in terms of personnel reductions or changes in operating methods, that department should be held accountable for it. So, this combination of user accountability for benefits and post audit to see that they occurred, I think is one powerful tool.

Don: If you were a GAO auditor reviewing a large computer system with extensive data communications links, what type of computer background would you want in the make-up of your audit team?

Ted: Well at a minimum, I would hope there would be a knowledge in the team of the typical points in the software, the hardware, and the communication networks where errors, losses or vulnerability to fraud, have been known to occur in the past, and the auditor then with that knowledge, can check all of the sensitive points, verify that the user is aware of them, and that reasonable precautions have been taken against problems arising.

Don: We hear a great deal about the seriousness of computer crime and the vulnerability of the computer to such deeds. Is this vulnerability a failure of the technology itself or a lack of management competence on the part of those who are responsible for the operation of the computer system?

Ted: Well, there's no question this vulnerability results overwhelmingly from a failure to exercise proper management oversight over what the system is actually doing and over who is actually using it for what purposes. The technology has little to do with it.

Don: We hear that the cost of data storage hardware is dropping more rapidly than other costs in data processing and that it will be cheaper to store data in computer files than on paper. Would you please discuss this, and what do you think the implications of that might be for government operations.

Ted: Well, I think that statement considerably overstates the case. In fact, during the next decade we forecast that computer storage costs may drop by a factor of a thousand. But if one checks that, he finds that it is still much more costly than paper. Also paper turns out, from our studies of the behavior of people in offices, to have many virtues as a portable, convenient means of storage. So maybe what will happen is that current information data, text and whatever, will be in the machine until the currency has passed, at which point paper will be used for official purposes, archival purposes, and informational purposes.

Don: We also hear about the potential value of computerized models as a means of assisting decisionmakers. Have you seen much of this?

Ted: Some models have a common problem that they must always contain some assumptions and generalizations, and they are unable to cope with the unexpected future event. Therefore, they rarely are able to predict the future precisely. But there are a considerable number of planners and managers who are using what are termed "what if" models--models in which they usually themselves have participated in making the assumptions, so they know what the weaknesses are; and then they will ask a variety of questions about the outcome of possible actions, receiving guidance as a result and perhaps proof against making serious error. This will guide them in their actual decision; they'll usually ignore the quantitative predictions made.

Don: It has been said that the Federal Government's inventory of computer systems is becoming obsolete. Do you see this as a problem?

Ted: Yes, I do. I have enough personal knowledge of the problem to believe it's serious. The Federal Government has laudably attempted to save money by using purchased computers for a long period of time, but I believe that in many cases it has incurred excessive personnel costs in doing so. For example, this new automatic easy-to-use software which will save much people-time over a period of years will not run on the old computers.

Don: Let's talk about productivity. Will you discuss for a moment the type of productivity changes we should be seeing in government as a result of the technological advances you have described for us?

Ted: Yes, I think broadly, people in offices at all levels from manager to clerk should have to be spending less time searching for, communicating, and manipulating information that's already been captured once in its raw form. This means that many man-hours should be saved in terms of basically useless behavior and also that current and accurate information should be available in a more timely fashion to all the people who need it.

Don: This has been a fairly short discussion about some of our main areas of interest and concern. To cap it off we would like to hear what you think will be the single most important change you expect in the next 10 years?

Ted: I think perhaps it will be that by then people will be accepting, no matter what their job or position, assistance from computers in many of their daily activities, not only for data, communication, and manipulation, but also for activities associated with voice, and text and graphic image manipulation and activity. For example, here we are preparing a visual communications, and I notice that there is a minicomputer dedicated to the control of this system, I think that's a foretaste of the future.

THE INDUSTRY VIEWPOINT ON ADP

by

John L. Jones  
Vice President of Management Information Services  
Southern Railway System

February 13, 1979

## Introduction of Jack Jones by Walter Anderson

John L. Jones is Vice President of Management Information Services, a department of the Southern Railway System in Atlanta, Georgia. He received a B.A. in Mathematics and Physics from Luther College in 1950 and an M.S. in Electrical Engineering and Mathematics from the Massachusetts Institute of Technology in 1954. In December 1974, Mr. Jones completed the Advanced Management Program at the Graduate School of Business of Harvard University.

From 1951 to 1957, Mr. Jones was in the United States Air Force and served with the USAF Comptroller in Data Processing and assisted in assembly and check-out of the first three UNIVAC I's. He was in charge of the Engineering Division Computer Center of the Chrysler Corporation from 1957 to 1959 and concurrently ne was a Management Consultant in Data Processing to the Air Force Logistics Command in 1958 and 1959. In 1959 he became a full-time civilian employee (GS-15) with the Air Force Logistics Command, responsible Command-wide for programing systems and standards, EDP equipment evaluation and selection, management of installed equipment and data systems research. In 1963, he became Assistant Vice President of the Southern Railway System with responsibility for all corporate data processing activities. In October of 1969, Mr. Jones was appointed Vice President of the newly established Management Information Services Department responsible for all corporate systems and data processing activities, including operations research and industrial engineering.

Mr. Jones is Chairman of the Executive Committee of CODASYL and a member of the General Committee of the Data Systems Division of the Association of American Railroads. In the past he has held positions of Chairman of the COBOL Committee; Chairman of the Data Systems Division of the Association of American Railroads; Vice President in charge of the Management Sciences and Systems Division of the American Management Association, and Chairman, Program Advisory Committee, Air Force Logistics Command.

Jack Jones

I suppose that most of you are amazed, even flabbergasted that a representative of a dying industry would be here to talk to you about such a fast growing field as computing. In thinking about what I could say that would be interesting and possibly helpful, I decided that the best approach would be to relate through case-studies what we've done at the Southern Railway System. You may be able to use that information where, and as you think, it applies in your own situation.

I'm going to try to touch on three different aspects of this problem. First, I will talk a little about the management style and the management environment in which this activity goes on in Southern Railway. Then I'm going to talk about the 8 to 10 principles that guide our thinking in terms of these kinds of problems, the designs of systems, and the chances we take or don't take, as the case may be. Finally, I'll give you a quick overview of a fundamental application--so fundamental that our chief executive officer has characterized it as being second only to the diesel locomotive in terms of effect on our corporate business.

I probably will tell you more about a railroad than you will ever need to know, but I think this may be an effective way to approach the problem.

The basic management style of the Southern Railway System is now, and has been for some years, a "democratic dictatorship." There's no question in anyone's mind in our company who the boss is. On the other hand, we have been able to develop a very open non-gamesmanship style which allows a broad discussion of an issue related to any topic by all the parties that could possibly be affected by the discussion. Sometimes, even those persons who aren't affected, but who are part of the management team, are included in the discussion.

I think that our style would be called that of a management team. The senior officers of the company have grown up in this style and therefore, on any given issue, will naturally call in all the members of their staff or anyone else's staff that they think might have something to say on the issue. After a thorough discussion on the issue, the responsible officer will make his decision based on his own judgment and determination, but having had the benefit of the diverse viewpoints that may exist. I emphasize, however, that the responsible officer makes the decision, and the majority doesn't rule unless the responsible officer is among them!

The way this process is applied to the computer field is fairly interesting. We have a committee on computer usage which was formed in April 1966 by order of the company president. It has met every third Wednesday of every month ever since then--almost without fail. Its membership consists of the 10 executive and regular vice presidents of our company. You might wonder how it is that the top officers--and it is a rare occasion that the president doesn't attend this meeting--find time or take the time once a month to discuss together issues related to the computer activities. That's a very simple matter. Our president just says, "Ya'll get together once a month and do this, y'hear." We understand that kind of guidance. The committee reviews every issue, every project, every report, and every new copy of an existing report that anybody requests be computerized.

The requestor must fill out a form which asks two questions, "What do you want, and why do you want it?" The questions are stated just that way on the form. The requestor has about 2½ inches of space to answer these questions. The requestor works with the programing staff, usually to get some estimate on the cost of it.

Once completed, the request is submitted to the 10 members of the committee. Each of us has 10 working days in which to vote on that request. So the requests from marketing, from sales, from accounting, from operations, law, and personnel, from everywhere, all get written up and sent to the 10 top officers--not including the president. The committee must vote unanimously to approve the project.

It may be a big project; it may be a little project. But no new report is added to the computer without this kind of writeup and review. If any of the 10 members votes against the project, or says he doesn't understand it, the requestor can bring anybody or anything with him/her, but he/she must appear to answer any and all questions regarding the request. This procedure has several beneficial effects. The first is that, as a result of this going on for 12 or more years now, the senior management of our company has become extremely aware of everything that is done on the computer and how the computer does things. We hear a lot about having understanding and participation of top-level management in these kinds of questions. My experience is that not only is it an essential thing, but it is absolutely critical to making good judgements not always based on the tangible aspects of a question.

A second good aspect of this is since very few people in our company want to appear before the president and the 10 vice presidents and look not to be particularly astute, the requests that come forward are usually well thought-out as to what is wanted and how they are going to use it. The third considerable benefit of this, from a personal point of view, is this leaves me in the situation where the corporation has decided what is going to be done on the computer, and it's up to me to decide how it's going to be done.

This is one of the many areas where, at least in Southern Railway (and I suspect in a lot of industries) you have a totally different situation than in the Government. The rest of the corporate team wouldn't think of asking me, "Why did you choose Burroughs instead of UNIVAC, or instead of IBM? Why did you get four megabytes of memory instead of three megabytes? Why do you have 22 spindles of disks? Why do you have six channels? Why do you have two machines of this size rather than a big one of that size?" They wouldn't think of asking me those questions. If they did, they might share part of the blame if I get it all fouled up! More seriously, they assume I'm part of the management team and will provide results in the most efficient and effective manner I can.

The question of what is going to be done is a corporate decision by all of the senior officers of the company. If it's a marketing application, everybody still gets a vote on it just like any other application. My job is to deliver what I promised within the cost that I promised it would take. If I do that, I'm a wonderful fellow with a white hat and the rest of the management team doesn't care how I did it. If I don't do that, I'm a terrible guy with a black hat, and they still don't care how I did it. They'll find somebody who knows how to wear a white hat.

So this activity has been going on for many years and it's important that you are aware of it because a lot of what I'm going to be talking about in terms of what we are doing with these machines is based upon the fact that there was management understanding, participation, and judgement involved in this.

As an example of the kind of thing we do in this committee, let's say there is a process proposed--possibly a new way to do purchasing, or a new technique to run a railroad yard, or a new way to measure the effectiveness of our distribution of empty freight cars. We will have the requestor come to the meeting and do what we call a walk-through. A

walk-through is nothing more than starting from the beginning and telling us where all the information is coming from; who is going to do what; how it is going to be processed; what the outputs are going to be; who is going to do what with them; and what the end-result of all this is going to be. Unless we all understand it, it just doesn't get done. It's got to be explained in one and two syllable words that we can all understand. As I said, everything is done unanimously by the vote of the 10 members. (That isn't always true. The president is not a voting member of the committee, but sometimes we lose 11 to 10 nonetheless.)

I would like to cover a few of the basic principles that we try to apply in looking at the things we are doing on the computer. One of the overriding principles that we have learned to apply is the principle of common sense. It's as simple as that--if it doesn't make common sense, it doesn't make any sense. The people sitting in this room didn't get to the positions they are in without having common sense and good judgement. There is no magic in that old computer box.

I think a second very important thing that we look at is whether or not the solution (the process) has been tailored to our specific situation. Vendors and consultants will tell you data is going to solve your problem, distributed processing will; if that doesn't, centralization will; if that doesn't, decentralization will. But, there are no pat solutions in this business. You must adapt the solutions to where you find yourself.

I already hit on the idea of management understanding and participation, and I won't belabor that except to say that it is terribly important. One thing we do which is, I think, very different and that is we always try to build a solution from the bottom up. We try to be modular; that is, pick out the kernel of the problem, solve it, and build on that base.

One of the problems you have in the Government is that everything you do has to be preceded by an extensive feasibility study. A feasibility study is a long-time look at a problem often getting down to nitty-gritty details like, "There's going to be an overpunch in column 72." You know it takes a long time to put together such a detailed justification. In my view, by the time you get done with this 1- to 2-year feasibility study, getting everything written

down and so on, and then go out for equipment selection, the problem has changed tremendously. It looks to me like a terrible problem.

When we think we have a big problem to solve, we pick out the smallest, "homeliest" piece that we can put in, get it running, and learn about it from experience--as opposed to soliciting the opinions of all the "experts" who never quite did it. We then add modules to this kernel, what finally is to be a large process. We make some mistakes. We go back and tear out part of that metal, unbolt it, rebend it, and bolt it back down. But we have the flexibility to do that. We can go back to the management in a form of our computer usage committee. If I get something messed up, I'll be first in line at the meeting to say, "Look fellas, I don't know how to tell you this, but I got it all messed up. Here's how it's messed up, and here is what I'm doing to fix it." That open communication is something that is also a real problem in Government.

I believe you ought to be very straightforward in the way you design things--the more simple, the better. I think you ought to--whenever you can--use off-the-shelf hardware and off-the-shelf software. You should never try to invent anything new in terms of hardware and software if you don't have to.

You must involve the user. If, when I get done working with a user department in our company, the user is not willing to step forward and answer the questions of the computer usage committee, it's "no deal" as far as I'm concerned. It's got to be the user's system. The user must decide how things are going to work.

Another thing is terribly important--always have a retreat position. No matter how carefully you've planned, no matter what precaution you've taken to make sure nothing goes wrong, something will. You need to know ahead of time what you're going to do when it does go wrong.

Now, I'd like to turn to a discussion of one of our basic applications. This system is right in the middle of being installed. I pick it because of the impact it will have on our company. It involves large central computers, mini computers and micro processors in fairly large numbers, and a rather massive communications network. It is the basis that we are using to gather all the data for operating the railroad. This is not some monitoring system. This is not some bookkeeping system. This is the basic system by

which we run the railroad at those points where it is installed. It is the system that our chief executive described as being second only to the invention of the diesel locomotive in its impact on our business. It is the system that causes the president or the chief operating officer to call me every once in a while at the wee hours of the night or early in the morning and say, "How come it is that I gotta look at your morning report before I look at my morning report?" So, it's a gut system in our business.

Briefly, the Southern Railway System covers about 10,500 miles of track in the 10 Southwestern States. We operate 600 to 700 freight trains a day. At any given instant, we have 70,000 to 75,000 freight cars somewhere on our tracks. We operate a large number of yards and agencies.

The thrust of this system has two basic concepts which center on the ideas that (1) when a person creates information, we ought to capture it and never have to capture it again. Source data entry is what that's called. It's not keypunching--a clerk sitting down and keying something from a document. It is that act of causing somebody to do something in such a way that when they do it, the data is automatically captured. Whatever it is they're doing, whether it's running a keyboard or issuing an order, they're not doing it for the computer system. They're doing it to get their job done. They have an incentive to do it accurately, timely, and completely. I say incentive because I know different folks need different strokes. However, the railroad is a very militaristic organization. We don't hesitate to look somebody in the eye and tell him/her to take an unpaid vacation for a few days or get going all together.

We're very tough on discipline in Southern Railway, and as a result, most of our people do have some incentive (even if it's not magnanimous) to get their jobs done accurately, timely, and completely. You must have these three things. If you don't, the computer can't help you. A computer doesn't back up the clock. If the person gets data into the computer an hour too late for the data to be used, the best the computer can do is get it to whoever needs it in an hour plus a few microseconds. The computer doesn't back up the clock. The computer won't take bad data--inaccurate data, and make it accurate. The best thing it can do with bad data is detect it and cast it away. Unfortunately, it usually lays it all out there for everybody to make mistakes with. So, disciplined source-data capture has to be designed into the system. The computer can't do it for you.

The other concept which is very appropriate for us (not necessarily appropriate for everybody) is one of those popular buzz words which everybody calls "distributed processing." I hope to give you some idea of what it means to us. Very simply, distributed processing is storing the local data and doing the local processing locally. It is not having everything sent to the central processor. The only data that goes back and forth between the central processor is that which is common and must be shared. You have to be very careful centralizing a large system such as the one I am going to describe shortly. If you have a system that is complex but not critical to your business, you can centralize it. Then when you have a crash (it's not a matter of if, it's a matter of when) it will take you a while to figure how to fix it. If it's not critical, you have time. If your system is very critical, but not complex, you're probably all right with a centralized system. When it crashes, you have to fix it right away. If it's not complex, you can usually figure out what's wrong. Unfortunately, systems don't come in vanilla and chocolate; they are in shades of grey too.

Systems tend to get more complex and more critical. Now, when a system crashes, you have to fix it right away because it is critical and you can't figure out what in the world is wrong because it is complex.

That is a situation which, in my case on the Southern Railway, would lead to a change in career patterns. That's one of the motivations that drives me in this way.

The system, very simply then, is one which tries to capture all the information about what's going on in the Railway--an example of one such data stream is a process we call "waybilling". In waybilling, our agent creates a document that moves with its related freight car. The waybill is so important to us that it is right even when it is wrong simply because that's exactly what is going to happen to the car. It's the only thing that exists; that one sheet of paper that gives us all operating information.

Another example is our automated yard inventory system which automatically reports train movements to one computer. This also includes all the movements of cars to and from industry, and of those to be exchanged with other railroads that we physically connect with at 240-some places. Cars are also sent to and from repair tracks and storage tracks. All these movements are needed for either local supervision or for central supervision. Our system is designed to capture all those movements on a source-capture basis.

I should point out that the system I'm going to talk about is one that we have been installing for about a year. We have about a year and a half to go to get the rest of the pieces together. However, this is second generation of such an online or realtime system.

Our first system to keep track of all the freight cars, all the trains, and so on, was installed in June 1965. So we have about 14 years of experience running this kind of online system. I can tell you a lot of interesting stories about the old version (some of them funny and some not so funny) but I think what is important here is the way we are transitioning into this new system and what the benefits will be.

We call this information our Terminal Information Processing Services (TIPS). This is the only computer system we have in Southern Railway that has a name. Here, we're talking about a railroad terminal, not a computer terminal. The individual who really made this work was a crusty old railroad man who learned what the computer could do. He almost single-handedly brought about the success we had in terms of the local changes--the operating changes that had to be made to make this system work. The name of the system is this man's nickname. The basic idea is that we wanted to make the job of our people easier. We also wanted to increase their productivity. As a by-product of them doing their normal job, we wanted to capture the information. This again is the source-data capture idea.

Let me give you a few definitions. We have both agency and yard personnel. Agency personnel are basically our agents. They talk to the customers, arrange to pick up the shipments, arrange for the billing instructions, and so forth. Yard personnel perform the switching and cause actions to occur in the yard--assembling trains, switching trains, etc.--two different functions. The yard receives the inbound trains, reswitches the cars, and produces the outbound movements. These movements may be to industry locations, or to interchange with another railroad, or another train. That, basically, is all a yard does. A terminal includes all the surrounding area: could be a few or many industries that receive cars from the yards. They load or unload the cars and return the cars to the yards. When we talk about the terminal area, it's all the industry around the railroad yards.

In 1973, at Sheffield, Alabama, we implemented a yard control system in what was a rather revolutionary way (at that time) by using five mini computers. These mini's did all the process control, including handling switches and controlling the speed of the car. This involves extensive instrumentation. They do all that work, plus keep all the inventories of the yard, and communicate with the Atlanta center as to the cars that are coming in and going out. Basically, the people in that yard sit and watch closed-circuit television to make sure that what they see (on the television) is happening is in step with what the computer thinks is happening. We achieved an increase in productivity of 40 percent per employee in that yard. This is a rather substantial increase.

Another type of yard, such as our pilot project yard at Savannah, Georgia, is a flat yard. It has the same basic elements of a receiving yard, a forwarding yard, and classification tracks. However, it is a lot more complicated because we switch from both ends of the class yard and on two tracks from either end. We were able to substantially reduce the labor intensity at that yard by the implementation of that system.

The next step on the mini computers was to implement the waybilling process. This was in support of the agency preparing the waybills. The next was to implement a terminal inventory, covering all the rest of that terminal area and the miles of tracks, docks, and industries around it. There may be 800 to 1,500 cars out there at any time. Our objective was to go to the spot on the tracks, on which track, at which door, and at which plant on which track each car in that area was located. We completed that in about mid-1977.

There are four major functions in this TIPS waybilling system: the yard inventory; the terminal inventory; demurrage (which is just keeping track of when the cars are at industry in the field to bill the customer for detaining the car), and finally the waybilling process. These are the functions done in the terminal.

Basically, that is what a yard has to do. It just gets back to keeping track of where they are and when they are moved. From that, we are able to give work standards to the industry crews that are switching these cars. The demurrage function is mainly a billing type of function. It is a by-product of the other operations allowing us to reduce manual recordkeeping.

In waybilling, that is a real gain. We have done a lot here to increase the agent's productivity, but nonetheless the basic idea is that the source data is captured by virtue of the agent preparing the waybill on a CRT with immediate computer edit and capture of the data.

Now, I want to get to the idea of centralized versus distributed processing. We presently have about 60 mini computers installed--and about 45 or 50 to go. We now have about 100 microprocessors and 154 more of these to install. They're all made by Data General. I make that point because we got started with Data General at the Sheffield yard. When we went to the Savannah yard, I picked Data General because we knew it. When the project was increased to go system-wide, we kept to Data General units and did not go out on a large selection evaluation. It looked to me like those units were about as good as anybody else's--not much better; not much worse. The price was about as good as anybody else's too--not much better and not much worse. It didn't look like it would make a lot of sense to study something like that for 6 months--something that looked like a waste of time and money. I make that point because that's a flexibility we have that obviously is a bit of a problem to you in Government.

In Atlanta, we have a network of four IMB 370/158's. Two of those at any time are doing batchwork; the other two are for online processing. Currently, there are about 20 communications lines, of which about 15 presently are on our own private microwave. We have a very large private microwave system. As a matter of fact, only AT&T and General Telephone have bigger microwave plants than we do. There will be 39 TIPS locations, 45 waybilling locations, and 182 microprocessor waybilling locations that will be connected to the Atlanta computer by about 50 communications lines when the project is complete by the end of 1980.

This gives you some idea of the coverage on the Southern Railway System. Our implementation schedule gets us to the end by 1980--a rather ambitious schedule. So far, we are on the money with it.

I hope I have covered enough to give you a flavor of what we do. As I said before, if I have said anything that is worthwhile, it is up to you to translate it into your own business. That's where the payoff will be.

Thank you very much.

Jack Jones' answers to questions from the audience

Q: Who pays for the cost of new reports or applications that are proposed to the report?

A: I do, because of the way we manage this activity which is on a corporate-wide basis. In other words, when we decide to put in a new report, or new application, or to do something like the TIPS system which is a much bigger kind of thing, the whole thing is discussed and agreed upon by senior management. A request from the marketing department is not done just for the marketing department--it's done for the Southern Railway. That allows us to take a budgeting philosophy which basically says my responsibility is to provide the needed corporate services for Southern Railway. I budget for everything related to data processing. There are some advantages to that. When some user comes in and says he needs a new computer terminal (and he didn't tell me about it before), he and I are going to sit down and have a good discussion about how he is going to use it; what he is going to do with it; and what he is going to save by doing it. I may say, "Great, that sounds good to me" and "We will do it," or I may say, "I don't know, that doesn't sound quite right," or "I don't agree with that," and he won't do it. The user has an alternative then. He can appear at the next meeting of the Computer Usage Committee and say, "I told him this and I told him that and he won't do it." The Committee may say, "Jones, get at it."

But it's my responsibility to plan the budget which is reviewed in detail by the budget committee which has four executive vice presidents. They have all the major responsibilities. They look at every expense, every cost center, in every department in the company. You have to go there all by yourself with your own case and be able to explain every darn dollar of, in my case, the \$14-15 million budget. As a result, this gets scrubbed up pretty good and we know what we have.

I think the critical point is that everything is out on the table. There are no hidden games. If an exception has to be made, we have to go back and explain it. It is a very good environment--partly from the fact that the Southern Railway System is just a whole lot smaller than the GAO or the Defense Department. There are things we can do that you all probably just can't do. I think if you think small sometimes it helps, however.

Q: How do they decide to buy, lease, or use services?  
Do you have any special rules?

A: Yes, I buy. Again, these are some things I can do. For example, if I am going to install a new computer, I will take a look at it and say, "How big do you think that thing has to be to last me 5 years, 8 years, or some such figure?" I won't buy what I think I need now, or next year, or the year after that. I will buy what I think I am going to need 6 or 8 years from now. I will give you a good example. In 1969, we put in a complex of two IMB 65's and two 50's. Undoubtedly, I could have gotten away for several years with IBM 40's instead of 50's, however, that would have left me faced with an extra conversion with its associated costs. I wanted to have it installed for 7 or 8 years so I bought the larger CPU's. The only thing I don't buy is when I look at something and I say, "Oh, something better than that has to come along." For example, on that same installation, IMB had 2703 hardware communications gear, but something had to be better than that. I rented those and sure enough in about a year, Burrough came along with a better one which we bought.

Q: In a rail yard such as Sheffield, if you lose electric power, and all that radar and other equipment doesn't work, are your people trained to manually operate and support the system?

A: Yes, they are. In fact, there are three or four levels of fallback. Finally, we would have to call in some extra clerks and send in some supervisors because after you have a computer system of any kind installed for a while, people will begin to lose their former skills. If there was absolutely no power, they could not switch tracks manually because the switches are operated electrically. But, we do have a big diesel generator, and we do know to use that.

Q: You operate and control a lot of heavy stock with computers. What kind of backup do you have?

A: Well, on the railroad, everything is designed to be failsafe so if there is a failure, for example, the signals turn red and will not allow the train to go on. This type of failsafe philosophy is in everything we do on the railroad because safety is such a paramount consideration.

Q: What percentage of the information acquired locally comes to your computer in Savannah?

A: I would have a hard time saying what percentage. For example, when a waybill is made out locally, all that information goes to Atlanta because we are going to need that later on for billing the customer and a bunch of things. There is also a world of things that happen out in the yard. For example, in the railroad yard, when a train comes in, it might go onto the third receiving track and a particular car might be the fifteenth car on the third track. The Atlanta computer could care less. When the car gets switched, it might be the second car or the fifth car on the sixty-fifth track. Again, Atlanta couldn't care less about that. So there is a tremendous amount of information which is strictly local.

When a yardmaster wants some function to take place, the only way he can accomplish that is to turn to his CRT and key in, "Crew number so and so go to track so and so, get so many cars and take them to track so and so." Then out come the printed instructions to the crew. When the crew is done, they call into the yard office and say, "Work Order Number 12345 executed (as is or with these exceptions)." That's the end of it. There is a tremendous amount of detail. I would have a hard time saying what percent goes to Atlanta. An example of what does go would be in a local computer, for example, when a train goes out, the yard man keys in and says, "Train 12345 is departed". The local record is going to be totally wiped out because once the train is gone, the yard couldn't care less about it. Before the mini computer wipes it out, it transmits all the data to Atlanta about the outbound train. Atlanta says, "I've got it." Savannah wipes it out, and Atlanta passes it on to the next yard.

Q: I was interested in the emphasis that you placed on being careful about too much centralization. Also on capturing information at the point of origin. I have two questions. One is: How do you decide what information you are going to share with all of your terminals? The other question is: To what extent do you link the computers at the terminals with the communications system?

A: On the first question, that decision is one that is made primarily (but jointly) by the operating parts who are working closely with my department. There are actually cases when we say, "Well this data is local and we don't need it in Atlanta," and then later on we may say, "That was a mistake--we do need it for this process." Sometimes, we say, "No, they don't need that locally," but later on we may find out we were wrong. Fundamentally, we take a very conservative approach. Whenever in doubt, we don't send the data back and forth unless later experiences demonstrate the actual need. I think the key factor to everything we do is, we try to do sort of a minimum basic thing and then with some experience, learn for sure exactly the answer to questions like that. There is a lot of data at a railroad terminal that is of absolutely no interest to another terminal; so a lot of that data might never get to Atlanta.

On the communication--everyone of these 240 or 250 micro and mini computer systems (some of them are dual systems; that is, there may be two computers out there sharing the same workload) are connected at all times to a dedicated communication line. In Atlanta, a computer is polling all these circuits 24 hours a day, 7 days a week, asking them if they have anything to send.

There is instant communication. There is no dial-up, once a day or anything like that. It is all connected at all times. In fact, a person sitting at a CRT out in a railroad yard can make an inquiry anytime. If it is of a nature that the local mini computer doesn't have it, it will automatically go to Atlanta, get it, and give him the answer. He doesn't even know where that information came from.

In other words, that whole thing looks like one system. Logically, it is just one big system. Physically, the pieces are distributed out where we think it makes some sense to it. It is a little more forgiving that way because if the central site goes down, it would not put the Southern Railway out of business. If the central site goes down, the small computers can keep working--at least in a degraded mode and some of them without any degradation.

TRANSBORDER DATA FLOW

By

Malcolm B. Greenlee  
Assistant Vice President  
CITIBANK

February 13, 1979

## Introduction of Blake Greenlee by Don Eirich

The topics of the next two speakers are related to the Logistics and Communications Division's issue area of Federal Information Management. Our visitor, Mr. Malcolm Blake Greenlee, will address us on the subject of transnational data flow. This appears to be essentially a concern of the private sector at the present time, and Mr. Greenlee will present an industry viewpoint. Transnational data flow, however, looms as a potential problem for Federal international programs and activities. A U.S. policy on this subject has not, as yet, been formulated.

Malcolm Blake Greenlee is an Assistant Vice President, Comptroller's Division, Citibank, where his responsibilities include development of corporate policies for data centers, risk analysis, communications security, and privacy.

Prior to joining Citibank in 1969, he was a compatriot of ours, being associated with the Johns Hopkins University and its Applied Physics Lab for 11 years. He served as senior physicist and program manager for various systems.

He received his undergraduate degree from Purdue and a graduate degree from George Washington University.

He has published several books and holds several patents.

Blake has been generous with his time in numerous professional activities, and he served with us on a Federal task force on computer security sponsored by the National Bureau of Standards.

Mr. Greenlee is prepared to answer any questions you may have upon conclusion of his presentation.

Blake Greenlee

The subject of this paper is Foreign Privacy Laws, Bills, and Transborder Information Flow. The European and Nordic State Governments have been moving much faster in these areas than the United States. Virtually every law that is passed affects the movement or processing of data beyond the national boundary of the country that passes the law. In this maze of laws overseas, there are two general types of laws, although the types tend to overlap.

One type is what is called a "data base law." It focuses on the creation, use, disclosure, and registration of data bases. It is concerned with protecting the data, not the processing operation. The registration is with a governmental commission created for that purpose. A good example is the Data Inspection Board in Sweden. The second type of law is the omnibus law; it covers everything. In addition to the processing and handling of data bases (covered by the data base law), this kind of law focuses on the collection, use, transmission, and processing of data base information from the time it is gathered until the time it is purged from the system. Again, in most cases, systems must be registered. There are two U.S. examples of an omnibus law. The Privacy Act of 1974 is one. The first private sector privacy bill (H.R. 1984), introduced by former Representative Ed Koch, is the other. That was introduced, and it served its purpose well as a stalking horse to bring the privacy question to the fore and start debate.

Following are some features of these laws. First, overseas, the implementation of the laws and their administration is the responsibility of a well-defined governmental agency or commission. (Because there is not such a well-defined, centralized point in the United States, it presents a serious problem to those who would negotiate treaties covering transborder information flow. The United States looks like an amorphous animal to the people overseas, and they know not with whom to deal.)

Another feature is how very specific the laws may be in terms of their requirements, and the German privacy law is a very good example. It has an appendix that looks like an extract of a good auditor's checklist for examining the information going in and out of the data center. Under this law, one must ensure that nobody can leave with a tape, that the data is protected and that only the right people have access to it. It is very, very functional in its approach, almost procedural. The French law, on the other hand, sets up an agency, gives it broad regulatory powers, and then provides that regulations will be issued. Discussed later will be some of the laws that may come in the future (e.g.,

the pending Belgian and Spanish laws), but in essence, such laws as they currently exist leave much open to be defined.

The laws do have many common features. In general, there are limited requirements on a data subject for furnishing information. There is certain information which can't be asked of a person, or, in some countries, of a corporation. People must have the right to know about the existence of their name in the file. They must be able to retrieve the information that is in the file about them, require that incorrect data be deleted or corrected, and have obsolete data deleted.

A major stumbling block to treaty negotiation is the way in which the information handling policy of the United States is perceived by foreign governments. The very existence of our intelligence agencies is a problem for people from this country doing business in the Nordic States and in Belgium where those nations see no need ever for a government agency to have as much information on its people as do our FBI and CIA. They have a fundamental difference in philosophy (or a fundamental lack of understanding). Their laws place stiff requirements on governments and on businesses processing data. They must make known the existence of the systems. There cannot be a secret processing system. If there is a processing system in those countries that is required for a national security purpose, its existence at least must be made known, and in-camera, in Court, the records can be looked at by a judge. He will decide if national security information is really involved. And he must be convinced. The countries where this is the case are Sweden, Denmark, and Norway. They have taken freedom of information perhaps farther than some U.S. citizens feel can be tolerated in the environment that our country faces. There is a trade-off to be made.

The notification process as to the existence of the system generally requires the system be registered (again with a public agency), public notice be given either in the form of a direct mail advice to the people concerned, or through newspaper announcements. In some cases one has to obtain permission of the governmental agency to establish the file. Whether it is a new consumer product or it is a new government service, one must go before the commission and lay out plans for a new system before the equipment can be purchased, the data gathered and the new system put on line. This involves a public hearing. The countries that have this type of law, or who are contemplating it, lay that requirement on their defense establishments as well.

If, after being placed in operation, it is decided that the contents of the file or system must be classified, then that fact is noted at the proceedings and there is a formal mechanism set up to place that information out of the public domain.

One must maintain an audit trail on who has done what with personal data, and that audit trail must be accurate. In some countries a record of every access to the file, every modification, every deletion, by whom, with what authority, on what date, and to whom it was revealed must be maintained. These are all questions that have enormous impact on the way in which systems can be designed. Clearly, if one required too detailed an audit trail, the audit trail would become larger than the data base itself.

Some laws have what are called "technical control requirements" which range from the normal data center protection procedures, that we would all insist on, to the requirement, expressed in a phrase in the appendix to the German law, that "during transportation on a data carrier, the information must be protected from observation, modification, or deletion." (The word "transportation" is used probably because the enforcement comes under the railway agency by some strange quirk of their system.) The only way to give that kind of protection to data is to add a serial number to ensure that the transaction or message is not lost, and then encrypt it.

There are provisions for monitoring compliance in all of these countries. In all cases there are reporting requirements and regulatory agencies. In Germany, an employee must be designated as the agent for data security, and he reports simultaneously to (1) the local senior management (equivalent of the board of directors) and also to (2) the national data protection board. This is tantamount to paying the salary of the Federal auditor on a Government staff. Aside from the obvious problem of adding another name to the payroll (because the person is doing an auditing function which could well have been lodged in the audit department), another layer of bureaucracy has been added. The individual is likely to find himself placed out of the promotional stream simply because he must act independently. Being outside the authority of the company, he very possibly will upset some people.

There are penalties for noncompliance with all of the laws, both civil and criminal. The French law states that the penalty for noncompliance with the act is a fine of up to 2 million Francs (\$400,000 in U.S. currency) and/or a

few years in jail. That seems a bit draconian from a business standpoint for not obeying the law. The guilty may also lose the right to operate in the country.

Following is a review of the status of the laws in the various countries: The three Nordic states have data protection laws. The oldest one was passed in Sweden, having been in effect since 1973. It is a data base law. The Swedes have had many growing pains with the administration of that law. Members of their Data Protection Board indicate they are going to modify and update the law and make it a bit more stringent. In a sense Sweden has served as sort of a model country for those who have passed a data base law. Last year, Norway and Denmark each passed laws: Denmark an omnibus, Norway a data base law. But their laws also cover corporations in addition to individuals. They recognize the existence of a so-called legal person.

Among the countries one normally associates as being Common Market, Austria has a new law. It covers legal persons. There is a law pending in Belgium. (As an aside, civil libertarians who wish to have a good law for protecting citizens' rights might want to focus on the proposed Belgian law.) The Library of Congress has published a translation of it. It covers almost any way to access information about an individual. A national security wiretap, regardless of the reasons, requires a court order. The court order expires automatically after 2 weeks and the person whose line has been tapped is notified. With the computerized information in files, there is essentially no way one can keep knowledge of the contents of a file from an individual who is concerned with that file unless there are very specific problems such as a psychiatric problem, or what is euphemistically called a social welfare purpose. That is their catch-all.

France passed a law in 1978. Many of the regulations have not been published. The French Data Protection Board has been established. On the basis of discussions with them, there is some concern because of the lack of clear-cut definitions. Some of the problems with the French law and with some of these other laws will be discussed later when national sovereignty concerns are addressed. Germany has a law--a new law. Formerly, only the State of Hesse had a privacy act. The other states in Germany will be passing privacy laws later this year. Luxembourg has a law pending. The Netherlands' law is pending and the United Kingdom has what is reported to be a white paper in process or out.

A particular problem in the United Kingdom is the tug-of-war between agencies such as that between civil

libertarians and our Justice and Defense Departments. Their Official Secrets Act, passed during the First World War, gives the Government censorship authority which is astounding. It is regarded by most as protection for the bureaucrats. Newspaper reporters have had stories classified and held when they tried to query whether light bulbs were used in a building. There is abuse occurring there, a tug-of-war will go on, and the English will eventually return to more freedom in this area.

In Brazil, there is an organization called CAPRE, from which one must gain permission to import any equipment for data processing or computing, or to have data lines running from Brazil to another country. The regulations that CAPRE has established are primarily to ensure that no information processing is done out of Brazil without being absolutely necessary. In other words, if processing can be done in Brazil, one has to do it there. If one can process with Brazilian-made equipment, one must do so. If one imports equipment then within a reasonable amount of time, Brazilian based organizations must be established to provide maintenance (including, e.g., building spare printed circuit boards). We had to build a modem repair facility in Sao Paulo because CAPRE saw that the people supplying our modems did not move fast enough to upgrade local talent and to establish a Brazilian-based industry for the maintenance of modems. They were put out of business by the government. The Brazilians, with their form of control on imports, have forced--and it has truly been a forcing process--an upgrade of about 20-30 percent per year in the technical capability of their people.

Spain has both a bill and a constitutional amendment on privacy pending. The OECD has a treaty draft in preparation. For those who are interested, Morris Crawford, in the State Department, can provide a copy of the latest draft. The drafting group will be meeting the early part of March in Paris again. They are due to complete the treaty draft and present it to OECD by the first of July. OECD's target is to present it to the ministers of the countries concerned 1 year hence. It may take 5 years to pass. Its object is to harmonize the system requirements of privacy laws among different countries. How do you live in an environment with 10 or 15 laws? The OECD is hoping to solve the problem this way.

There are some issues that ought to be examined in the transborder information flow area. The primary force behind many of the privacy laws overseas appears to be national sovereignty. Foreign nations want to protect their citizens. Here is an example.

Imagine the reaction of a Frenchman on the street if one walked up to him and said, "Excuse me, sir, I thought you might be comforted to know that across the Rhine is a major computer center and in the event that their service is ever required for you, or your records lost, they have your name and address; they have the names and addresses and medical histories of everyone in your family; they have information on your race, religion, your political affiliation, and oh, yes, all your financial transactions." Imagine what thought would run through that Frenchman's head. Memories are long. Manual files in existence in European countries at the onset of the Second World War were the primary tools used by the German government in picking up control of the nations they conquered. How much easier it would be with computerized records. So there is a desire by these countries to keep their files at home, keep their citizens' information where they hope they can control it to protect their citizens.

Foreign nations also want to protect their economy. They do not want jobs exported. Their rule-of-thumb is if they have to process, they process at home unless there is no equipment in the country with which to process. If one examines the thrust of the privacy laws and the differences in them, one quickly concludes that in the long-term it is cheaper to decentralize processing and process on a country-by-country basis. To centralize processing in one point, say for all of Europe, would render the programming job and the subsequent accounting and control job absolutely unmanageable. These nations also worry about outside intervention in their financial affairs and in the affairs of their countries. They do not want a data base on a computer in another country that affects a major part of their economy where access to that data could be denied by a local disaster, by a strike, or by some other intervention. They worry about disruption of data processing communications passing across other nations.

The Germans do not want processing interrupted in a German bank, or in a German business, because the data base is in Belgium and the line passes across France, and if they get into a squabble with the French over a border dispute, somebody cuts the line. These are defense and intelligence related issues.

One should make the tacit assumption, if one is engaged in private business--in any kind of domain--that communications are being monitored by the countries when those communications cross their borders. There is a hue and cry in foreign lands about people tapping phone lines when they go in and out of the country, but in fact in most countries

that is a primary way for the government to monitor and control the activities of foreign nationals and foreign concerns doing business in their environment. They are also worried about outside intervention in their economy and its disruption.

When businessmen complain about the difficulty in complying with the laws, the answer is simple. And that is to remember that, in doing business in a country, one is a guest there and will remain so as long as businessmen obey the laws willingly and there is a spirit of cooperation among them. The same will hold true for any U.S. Government computer installation in a foreign land. For example, in a U.S. payroll system in Europe local citizens will be part of that payroll. Europeans will not allow the data to be sent back to the United States for processing. They will want to keep it in Europe. They will monitor what is sent on their lines. There are valid national sovereignty issues involved, and in many cases, they are of much more concern to the Europeans than privacy.

In the economic area, preservation of jobs was discussed. Some countries commit themselves to a fixed unemployment rate, others to a fixed rate of growth. No country, especially those that are called third world or developing countries, can afford to export high technology jobs. The pressure is on and will be on to keep those jobs at home. If one is planning to install computers, they should be installed locally. Only that information that is required outside of the country may be transmitted. Similar to the situation illustrated in the fine case Jack Jones cited in automating the railroad yard, any information that is not needed at the central computer site is not sent there. It is handled locally.

The next point to discuss is that in a short period of time there will be pressure to use equipment produced within the country. That is particularly likely to occur in France because of the broad structure of the law. The French regulatory authority can easily mandate that one may only process personal data on a computer whose operating system and whose hardware it has certified, and whose hardware manufacturer they have followed through the plant to make sure no one has placed any connections, wiretaps, or whatever, inside the machine that would cause the rights of its citizens to be jeopardized.

What I believe that the French and others are really saying is: "Use our equipment, but don't export our Francs, Deutsch Marks or our Cruzieros to another country. Process

here with our people. Train our people. Don't bring outsiders in and don't ship the data outside our country or process it outside the country."

There has been talk about putting a value-added tax on data. That concept originated with the late Mayor Daley of Chicago as a result of a dispute with the State Banking Commissioners in Illinois. Illinois is a unit banking State. Only one bank location is allowed--one office, one physical location, no branches. The banks in Chicago decided that they would like to put cash dispensing machines a few hundred yards to a few miles away from their one legal office. Mayor Daley said that he would go along with that. He would introduce not "State's Rights" but "City's Rights," and he declared that the City of Chicago had the authority to regulate its own banking (within limits, of course) and would allow the banks to install the terminals--of course, subject to a tax--(a fraction of a mill per bit) based on the data transmitted.

The outcome of this was that the courts quickly disapproved of this venture (and the income to Chicago), but the concept of a value-added tax on data was soon picked up by others. It is now written into the customs regulations in the common market countries. If a tape is brought into a country, the duty on the tape is computed on the basis of the value added to the tape as a result of storing the data, writing on the tape, the value for that one use of the computer utility, plus about 15 percent for G&A and profit. The data itself is not taxed, but what is taxed is the value added due to the processing.

Restrictions are coming for private networks. The U.S. Government has its own private switching networks as do most major multinational corporations. Private networks make it easier to control Citibank's business as they do for the Government. But in a sense, private networks represent revenue loss for the carriers overseas in the overseas countries. Business is experiencing much pressure now not to install more private lines. Probably the Government will find it more and more difficult to get leased lines/private lines overseas. It may have to pay the higher rates for the normal Government service.

Another issue is consistency. There is absolutely no consistency among laws in the various countries, and the situation looks like an impossible maze. However, from the point of view of a pragmatic businessman looking closely at the impact, it will be found that no two countries have the same accounting laws, tax laws, or labor laws. Doing businesses in many countries requires compliance with

differing requirements in different places. With this in mind one can take the laws and strip out the features that are different among them to find a common base for all of them that involve those citizens' or data-subjects' rights that were discussed earlier.

There are two approaches to privacy laws. In the United States laws are based on English common law and the individual generally must step forward to protect his or her rights. If someone does something which another doesn't like, then one can go to court, get an injunction, and sue the person (except in certain specific cases where something has been defined as illegal, such as wiretap). European laws are based on a legal code. A socialistic approach is taken. The state is relied on to control aspects of people's lives. The individual should not have to assume the initiative about going to court to sue people to stop them from interfering with their rights or modifying their data in the file or using incorrect information about them. In general, the United States passes laws to counteract very specific problems--what some people call a rifle-shot approach. In foreign lands the laws tend toward omnibus laws: they are general-purpose. They aim a shotgun in the general direction and try to solve all problems at once. One system of laws is not necessarily better than another. It's just that there are vastly different approaches to handling the same kinds of problems. One must understand the differences among the countries on this.

As was mentioned earlier, there has been a problem with the lack of a formal U.S. policy. For the past year there have been negotiations in OECD. The first question facing the U.S. representatives when they arrived at the drafting conference to draft a treaty to harmonize the effects of these various privacy laws was, "How can you come here and sit and help us draft a treaty when your own country doesn't know in what direction it's going?" The basic problem is that there are conflicting interests of law enforcement agencies and civil libertarians, and those have to be resolved. Foreign nations also do not understand that the United States has a constitutional structure which incorporates the concept of States Rights. In December, the U.S. Government hosted, in New York, a meeting of the members of the Data Protection Boards from virtually all the European countries, the Nordic states, and people from the OECD. People from State, Commerce, the FTC and Justice presented views on privacy protection in the United States. And a point that surfaced and absolutely floored our European counterparts was that unless a system is used in transporting data or processing in interstate commerce, it is outside of Federal law. They had no earthly idea that there was such a restriction on the authority of

the Federal Government. In discussing international processing of data that doesn't apply, international commerce is obviously interstate commerce, but it still points out a basic lack of understanding between the way our society functions and the way their society does.

The primary concern of the people overseas, which appears to be quite biased, is that they see the U.S. Government as having much, much less concern over protecting the rights of its citizens than they think they have in their own countries. However, every one of those countries also has its intelligence service which has been neatly excepted from the law (all but the proposed Belgium law which has broad application). They have their national defense and national economic issues which require, for the protection of the country, that some information be screened. This is an area which is experiencing a great deal of change, a great deal of flux.

In the United States, at last count, there have been over 6,000 privacy or privacy-related laws introduced, but the United States is still behind. The U.S. Government and private industry still have to face the fact that they will be dealing with a different law in every country on this for some time to come. The indications are there. Laws are in place. The approach inside Citibank has been to cease all theoretical study of foreign laws. It is not a study problem; it is not a job for consultants; it is an out-and-out operational compliance issue. Citibank's approach has been to give copies of the laws to the operations management in the various countries, introduce them to the local counsel (if they need introduction), provide training for their auditors in the aspects of the law, and start auditing for compliance. This is going to hamper operations in a couple of places for a while. It will affect long-range business strategy. There will probably be fewer and fewer multinationals installing large, centralized computing installations. Decentralization is going to be pushed and enforced by the law.

## Blake Greenlee's Answers to Questions from the Audience

Question: You mentioned that one of the problems that the United States has is that it has no national policy on privacy. Would we be in better shape if we had one?

Answer: I think that we can achieve the same end results without an omnibus national law and without another regulatory agency. We only have 82 that we deal with right now. But without a centralized point in the U.S., Europe sees no way to communicate with the U.S. on a potential privacy problem. They see an agency needed as a point of contact. They understand that Regulation Z or the Truth-in-Lending Act would protect some things, that banks have been assisted in controlling the flow of subpoenas through their doors for customer information by the Banking Act of this last year. If you go through State by State, law by law and through the various Federal governmental agencies, we've got a lot in place that does exactly what the foreign laws do, but we don't have a centralized authority. They see that as a problem and they don't understand; they really don't understand, our approach to solving specific problems with our system of laws--as opposed to implementing a new section of legal code. It is really a difference in philosophy and mind-set.

Question: You pointed out one of the problems in this country is to decide what type of access system in data banks is needed for law enforcement. Can you generalize the situation in Europe?

Answer: In general, the Europeans, and I mean no slur, on the surface are very pious about the fact that they treat their citizens' data very nicely and then they point to the Privacy Protection Study Commission hearings that reveal our abuses (and they have to be called abuses by some of our law enforcement agencies in getting into information, data bank--some of the stuff that went on in modification of credit records, for example, with the American Socialist Workers Party). They point to this, wave banners, fire guns into the air, and say, "That's an intolerable situation. You have to fix that before we can allow data to be sent back and forth," when in fact they have law enforcement agencies which have much broader powers than we have here. (As I said, Belgium is an exception.)

## SLIDES USED BY BLAKE GREENLEE

### BACKGROUND

- o European and Nordic state governments have moved much faster than the United States in passing privacy laws.
- o Virtually all these laws affect movement of and processing of data beyond national borders.

### GENERAL TYPES OF LAWS

- o Focus on "DATA BASES"
  - Creation
  - Use
  - Disclosure
  - Registration
- o Focus on processing of information (so-called OMNIBUS LAWS)
  - Collection
  - Processing
  - Use
  - Transmission
  - Registration of systems

### GENERAL FEATURES OF FOREIGN PRIVACY LAWS

- o Implementation/Administration is responsibility of governmental agency or commission.
- o Laws may:
  - Be very specific in terms of requirements (Germany).
  - Give the governmental agency broad regulatory/interpretive powers (France).

STATUS OF FOREIGN PRIVACY MEASURES

<u>COUNTRY</u>	<u>STATUS</u>	<u>TYPE</u>
<u>NORDIC STATES</u>		
Denmark (1)	Passed 1978	Data Base
Norway (2)	Passed 1978	Data Base
Sweden	Passed 1973	Data Base
<u>COMMON MARKET</u>		
Belgium (4)	Pending	Data Bank
France	Law 1978	OMNIBUS
Germany (Federal)	Law 1977	OMNIBUS
Luxembourg (4)	Pending	Data Bank
Netherlands	Pending	Data Bank
United Kingdom	White paper to be issued	--
<u>OTHER</u>		
Austria	Law 1978 (3)	OMNIBUS
Brazil	Regulations restricting processing done out of country or by firms not controlled (50 percent owned) by nationals	--
Spain	Pending	Bill and/or constitutional protection
OECD	Treaty draft in preparation	Principles Guidelines Harmonize laws
Council of Europe	Draft resolution/ international on protection of individuals vis-a-vis automated records	--

(1) Covers legal persons; e.g., corporations.

(2) Export license required to send personal data across borders.

(3) Covers legal persons; e.g., corporations. License to export data required.

(4) May cover legal persons.

## SPECIFIC FEATURES OF LAWS INCLUDE

- o Rights of data subjects
  - Giving information
  - Know of existence of name in data base
  - Know and/or get copies of information
  - Require that incorrect data be corrected/deleted
- o Requirements on government/business
  - Make known existence of system processing personal data
    - Resistration
    - Public notice
    - Permission to establish data base
    - Audit trail on who has seen/modified data
- o Technical control requirements
- o Provisions for monitoring for compliance
- o Penalties for non-compliance
  - Civil
  - Criminal
- o Restrictions on sending data across national boundaries (explicit or implicit)

ISSUES IN TRANSBORDER INFORMATION FLOW

o National sovereignty

- Protection of citizens
- Protection of economy
  - Outside of intervention
  - Disruption
- Defense/Intelligence related issues

o United States policy

- U.S. negotiations have been hampered by a lack of a formal U.S. policy/position on privacy. Such a position paper/recommendations to the Congress are expected in early 1979.

o U.S. constitutional structure

- Foreign governments do not understand the limitations on powers of the Federal level of government vis-a-vis the States as defined by the Constitution.

o Economic

- Preservation of jobs
- Pressure to use equipment produced in country
- VAT on data
- Restrictions on private networks

o Consistency in law/regulation

- There is no consistency in the privacy laws pending or passed; they all conflict in one way or another.
- This situation is NO DIFFERENT than the country-to-country variations in
  - Labor laws
  - Accounting and tax laws.

o Approach to privacy legislation

United States

- Based on common law
- Rely on individual to act to protect rights
- Laws to counteract specific problems

Europe

- Legal code
- Socialistic; State is relied on to control
- General ("OMNIBUS") laws

## ACTIONS FOR UNITED STATES BUSINESS

- o We are guest in each country and must obey the law.
- o Treaties are 3-5 years off; compliance must be country-to-country.
- o Businesses can establish compliance policy based on:
  - Common features of laws.
  - Specific variations (exceptions) for each country.
- o Involve local staff
  - Legal
  - Operations
  - Audit
- o Appraise State/Commerce Departments of any problems.

PRIVACY PROTECTION AND TECHNOLOGY

by

Robert G. McKenzie  
Audit Manager  
Logistics and Communications Division  
U.S. General Accounting Office

February 13, 1979

Introduction of Bob McKenzie by Don Eirich

Our next speaker, Mr. Robert G. McKenzie, is an Audit Manager in the Logistics and Communications Division, where he is principal adviser to the GAO in the protection of personal and sensitive information.

He assists in the development of policy in this area and serves as a consultant to congressional committees, Federal agencies, and other GAO divisions.

Also, he was appointed by the Secretary of Commerce to Federal Information Processing Standards Task Group 15 on Computer Security. He is the task leader for development of Federal guidelines for Audit and Evaluation of Computer Security, and he served as Chairman of two National Bureau of Standards workshops on this subject.

In 1978 he received an award from the Washington Chapter, Association of Government Accountants for outstanding achievement in improving Financial Management.

Prior to joining GAO in 1974, he served for 20 years in the Air Force, where he pioneered in the development of audit approaches for data processing systems.

He received his undergraduate degree at Florida State and a graduate degree at Southeastern University.

Robert McKenzie - Summarized

Information, while intangible, represents one of our Nation's most important assets. It is precisely because of the criticality of information to the governmental process that agencies have, over the years, requested more and more information from the public and have pressed into use the most advanced technology for its processing and storage. The use of computer technology and the concentration of information has given rise to a growing public and private concern over the potential for misuse and the invasion of privacy of the individual citizen.

The concerns over privacy and related security issues have had an adverse effect on computer acquisitions, but the full impact has yet to be felt. This is because the various civil agencies are just now beginning to address their security requirements at a level above their basic physical security needs. However, there is still much to be done.

Most agencies have yet to implement an effective security program. In a recent report, GAO noted an absence of top management involvement, with a resultant lack of organizational structures, policies, planning and procedures which are necessary for funding, development and implementation of effective security programs. As long as these deficiencies exist, Federal agencies have no assurance that their computer resources and data are properly secured or adequately protected.

In our report to the Congress on "Challenges of Protecting Personal Information in an Expanding Federal Computer Network Environment," we recommended that the Director of OMB take the necessary actions to expeditiously provide the Federal agencies with comprehensive guidelines that: (1) contain the definitions and criteria necessary to permit an assessment of their security requirements, (2) provide the methodology to be used in conducting such assessments, (3) identify the physical, administrative, and technical safeguards that should be applied in satisfying their security requirements, and (4) specify the means to justify the associated cost.

The impact such guidelines could have on future procurements of computer hardware, software and services and on the manner in which they are used, is obvious. However, the question today is, what type of system can be obtained now that will provide a high level of protection for personal or other sensitive information. The report cited above discusses some of the threats to computerized data and a few of the system vulnerabilities. Also discussed is some of the technology that can be used today to provide a high level of protection for data in shared computer networks.

In examining the risk to information maintained on computer systems, it appears that the threats stem from two sources: first--authorized, but untrustworthy or dishonest users, and second--malicious penetrators. The untrustworthy user has authorized access to the data of interest, while the malicious penetrator does not.

Protection against untrustworthy or dishonest employees is indeed difficult. However, the risk can be substantially reduced through proper application of well-designed managerial controls, which include: segregation of employee duties, personnel screening, activity monitoring, and effective auditing. These and other managerial controls have been afforded extensive coverage in literature published over the years by universities, professional societies, and Government.

Malicious penetrators present a different threat than untrustworthy employees in that they must circumvent technical security measures. Our study of the views of experts in the field indicates that skilled individuals generally penetrate a system by using an operating system function in a way unanticipated by designers, or by exploiting some anomalous behavior of the operating system. They achieve their objectives by various methods, including (1) acquiring by any method a list of user identifiers and corresponding passwords, or (2) obtaining supervisory (executive or master) control of the computer system. Using the first method, the penetrator can masquerade as any of the authorized users of the system, while use of the second method gives him direct access and control of any file or program in the system.

It would appear that computer systems are extremely vulnerable; and indeed they are, but there are ways to reduce the risk. Today, it is possible to attain a high level of data security by (1) reducing the threat from those individuals with the technical training necessary to circumvent safeguards and (2) segregating sensitive data and its processing from all other data, hence adoption of a policy of isolation. There are a number of ways to implement such a policy including the development of transaction-driven systems and the use of such technologies as virtual-machine systems, descriptor-based systems, the kernel concept, etc.

While absolute security is, in fact, unobtainable, the proper use of current technology can provide a high level of protection for personal and sensitive information. It seems logical that further progress toward more secure hardware and software will be accelerated to the extent that management recognizes their security needs and places such demands upon the computer industry.

HIGHLIGHTS OF THE DRAFT CONSENSUS REPORT  
OF THE PRESIDENT'S REORGANIZATION PROJECT  
ON FEDERAL DATA PROCESSING

By

Alton P. Jensen  
Georgia Institute of Technology

February 13, 1979

### Introduction of Pete Jensen by Wally Anderson

Alton P. (Pete) Jensen has been active in the teaching and management of computing at the Georgia Institute of Technology since 1957. He has been principal investigator on numerous sponsored R&D projects and served as Chairman of Georgia Tech's Computer Advisory Board during the procurement of its current \$7,000,000 computer facility. In addition to his academic involvements, he has fostered the development of computing in business, industry, and government by participating in a variety of organizations as consultant and principal. In 1972, he directed the data processing component of then Governor Jimmy Carter's Reorganization and Management Improvement Study for the State of Georgia.

Pete Jensen has had a principal role in drafting the final report for the President's Reorganization Program for ADP. He is formally known as Professor Alton P. Jensen, Department of Computer Science, from the Georgia Institute of Technology.

Pete Jensen - Summarized Opening

In his introductory remarks, Professor A. P. (Pete) Jensen referred to his participation in the 1972 study of data processing in the State of Georgia. He and Jack Jones were team members of that study under the direction of then-Governor Jimmy Carter. Some 5 years later, in correspondence with Mr. Bert Lance, at that time, Director of OMB, Professor Jensen pointed out the need to bring substantial participation of the private sector into the President's Reorganization Project in order to give the private sector representatives an appreciation of Government workers and, at the same time, to let in fresh air from outside the Government.

Professor Jensen referred to the 55 people who participated in the study. Forty percent of these were from the private and university sectors. There were 10 study teams: 5 organized along agency lines and 5 organized according to topic areas. Each of the study teams operated on its own and provided a summary report of its activities, findings, conclusions, and recommendations. Professor Jensen, together with a small group from the study teams, worked to find a consensus in the 10 reports and to provide that information and recommendation through OMB, with comments, to the President.

In his introductory remarks, Professor Jensen also referred to the history of the Brooks Act, to correspondence from President Lyndon Johnson regarding its implementation, and to the many GAO reports used by the study teams. Professor Jensen indicated that one of the purposes of the Brooks Act was "to prevent sin" and that, since then, the "cost of sin" had been going down. He drew a diagram on the blackboard which showed the decline in its unit cost from 1965 to the present time as a result of the decreased cost of computer components. There was a corresponding rise, however, during this period in the "cost of preventing sin."

\* \* \* \* \*

Pete Jensen

The results and recommendations of this study are anchor points for improvements in the future. Early in the study, to our surprise, we found that the Brooks Act was a point of strength--something that could be applied and built on for the intentions and direction of this study. What needs to be addressed is how that act can be better implemented; how it can be better used in the future.

With that comment, I'd like to begin with a brief review of the consensus document as it exists. Please feel free to interrupt me and exchange ideas as we move along and see where the discussion leads us. I'd like to get feedback from you. I want to emphasize again that this is a draft document--still in the formative stages. It is, I hope, nearing completion. What I have to say, however, basically represents my own views.

This study has a distinction that some of the other reorganization programs don't have—it has had substantial participation from the private sector. Of the 55 people who were involved, over 40 percent were from the private and university sectors. The OMB is to be commended for having produced the study in an extremely open manner; I am sure this was accelerated to a large degree by the participation of the private sector.

Among the things that the report will reflect is some pretty harsh criticism of OMB. Among the things we wrestled with back in June was the matter of how our report would be submitted following the study. The agreement we have with OMB is that the report will be forwarded through them, with comments, to the President. This we consider to be a contractual part of the overall study, and we think it is certainly commendable of OMB that it took no action to either stifle or restrict any of the things we had to say.

We felt sufficiently good about the experience of the whole enterprise that we wanted to dedicate the report to the many courageous and diligent Government workers who have had to wait too long for the changes recommended. So this is the tone, the nature, and the direction of the report.

We would say further that this report, for all of the effort that has gone into it, does not present a large number of entirely new findings. We can look over the last 15 years of governmental activity and see study after study, recommendation after recommendation, that will map directly through everything that is being said here. We certainly want to recognize that we're not enunciating new problems and new recommendations; but what we do hope to proclaim (through the strength of this Administration and its commitment to change and improvement) is that action will finally be taken along these lines.

One of the problems that we struggled with early was the problem of terminology. The main issue is what, in Government, you tend to call "ADP." ADP has meant either Automatic Data Processing or Administrative Data Processing for as long as I have been in computing. We began looking for something else—since ADP is an out-of-date term that doesn't say anything and doesn't reflect the current confluence of computing, information, and communication technologies. As a consequence, we elected to use the term "information technology" almost uniformly through the report in place of data processing, ADP, or any similar term.

The term "information technology," as we have used it, refers to the current setting in which there is a confluence of computing, communications, and information concerns of the sort you have been reviewing here today.

In the course of listening today, I heard that Government has a natural tendency to emphasize oversight and control; I also heard some reflection on the notion that technology can be used to manage technology. Our report clearly recognizes the fact that if the information technology is to be managed, it must be managed through the information technology. This is, of course, one of the things that has made the whole business of computing as successful and as important as it is today: the tool itself can be applied to its own management and for the production of its own benefit. This is done through the use of high-order languages and through operating systems which make it easy to use computers. I developed a phrase a number of years ago: "using the computer to solve the problems of using the computer." We would like to see this notion carried further—we would like to use the technology to solve the new societal problems of managing the technology, whether those problems deal with the issue of privacy, with security, with administration, or what-have-you.

Now I will review briefly and comment on the nature of these findings.

Those of you who have reviewed the 10 reports that are in print recognize that it's impossible to put all the findings into one coherent document. We have attempted to condense the findings and still retain the spirit expressed across those reports.

Within that framework, we find, first of all, that the Federal Government is increasingly and irreversibly committed to the use of information technology to manage its resources, provide its services, and protect its citizens. Based on what we have heard here today, there is no question about that. It's not a trite finding. It's one that must be enunciated, underscored, and established as a priority within the enterprise of Government.

Furthermore, information technology can be an effective means of reducing the cost of Government, and may be the only means of expanding governmental services without increasing budgets. We have seen, in the private sector, that some companies (though, of course, by no means all) have managed inflation and its related problems by using computers to increase overall productivity. One thing becomes clear when you look at the Government, and that is that it is terribly undercapitalized with respect to equipment that supports the white collar worker. The data indicates that the ratio between the private and Government sectors (in regard to such support) is better than two to one. So we find the Government deficient in this area.

The accelerated development of and commitment to information technology, though not a goal in and of itself, is a means by which an information-intensive society may be able to achieve its objectives. If a railroad is information-intensive (that is what Jack Jones said this morning), certainly a Government is information-intensive. You can't manage a railroad without managing information and the Government is, if anything, in order of magnitude more information-intensive than a railroad. Information is the product—the substance—of Government.

To follow in with the phrase that Mr. Staats used earlier this morning, the Federal Government is, in general, mismanaging its information technology resources and has not developed a plan for exploiting the opportunities of the future with respect to investment, service delivery, or national security for protection of citizens. This condition is, to quote the report, "manifested by such major symptoms as public complaints about delays and inaccuracies at many service delivery points." This is probably the most profound understatement of all our statements. It's rather an emotional thing, particularly for the human resources study team. That group identified at least one program in which the eligibility determination process requires a longer period of time than the life expectancy of an eligible applicant--three hundred and some odd days, particularly in the case of black lung. This is a very emotion-charged statement and yet it is an understatement.

The report also finds that the Government has been unable to protect the rights and privacy of individuals or to deal adequately with a growing obsolescence of equipment, systems, and personnel; that there are increasing economic threats which have been accelerated by the availability of technical information and products flowing freely and uncontrolled from the United States into competitor nations; that we have a military enterprise which is operationally vulnerable as the consequence of obsolete equipment and systems and underdeveloped technical personnel; and that these major symptoms are principally caused by the apparent unwillingness of the Office of Management and Budget to exercise managerial, in contrast to budgetary, control over information technology.

There has been a failure on the part of the Office of Management and Budget, the General Services Administration, and the Department of Commerce to effectively discharge the responsibilities assigned to them under Public Law 89-306. In this regard, we had a number of interesting sessions with the group in the Central Agencies Study Team. One day we were sitting around trying to decide how we would summarize the report, and I think it was Licklider who went to the board and wrote, "OMB," "GSA," and then "DOC"; then somebody else got up and under OMB wrote, "do more," under GSA, "do less"; and under DOC, "do something." The last exhortation was in response to a problem that has been mentioned several times today: the abdication by program agency management of responsibility for managing information technology as a mission-oriented resource.

We found also that the intrusion of the legislative branch into the decision process of the executive branch, through avenues other than those of the General Accounting Office, goes beyond the scope of normal oversight. These are serious problems resulting from current conditions.

These summary findings indicate an urgent need to exploit and accelerate the application and development on information technology to (1) reduce the cost of Government, (2) improve service delivery, (3) protect our privacy, (4) improve our individual and military security, and (5) maintain world leadership in the technology that holds the key to a new era.

It is in the framework of that set of findings that we attempted to develop some conclusions. I could not help reflecting today, while Blake Greenlee was commenting on issues of transborder data flow, that during one of the reorganization project meetings I attended, the subject of transborder data flow came up, and the person that we were meeting with stated that it was not a serious problem for the Government at the present time--because it only affects industry!

But along this line, within the framework of our study conclusions, there are several dilemmas that have to be dealt with. The first dilemma stems from the fact that program managers must have the responsibility and the authority to manage their missions. These managers must have the authority to manage information technology in order to fulfill the responsibilities of their offices.

But the problem is that the program managers are not equipped to do that job. Either they do not have a mind set to doing it, or they are intimidated by the technology or by their technicians, or there is some other difficulty. And they end up abdicating their common managerial responsibility to information technology people who should not be making the decisions.

Another dilemma stems from the fact that the Brooks Law has clearly placed responsibility for the management of information technology in the OMB, the GSA, and the DOC. In its implementation, all three of the principal agencies have been substantially discredited with regard to their ability to fulfill the requirements of law. Changing the responsibility from OMB to GSA has not solved the problem.

This is a fundamental dilemma which leads to the question: what can we do about it? Clearly, moving the boxes--or reorganizing the boxes--will not make a difference. The substantive element that is missing is some level of commitment--a program of education for mission managers, for one thing, and, perhaps more important, an acceptance by the central agencies of a leadership role and of the responsibilities involved in such a role.

We attempted to make some positive statements in this regard. It was said that, with regard to the line agencies, the Federal Government must establish clear and measurable criteria by which mission performance can be judged and competence rewarded. When competence is rewarded, it is built and strengthened. This building and strengthening of competence is the major task faced by the Government.

I cannot avoid saying here that the information technology must not be singled out for special treatment. It must be treated as a resource to be used in accomplishing missions within the mission agencies. The agencies must have the competence to do what needs to be done.

With regard to the central agencies, the Federal Government must bring about a managerial revitalization--a revitalization characterized by the channeling of central agency effort into positive programs--programs

which provide the Government with energetic and knowledgeable advocacy of the effective use of information technology. This is the only connection in which the term advocacy is used in the report. We are told that advocacy is not a good term. We have been told that in Government, advocacy means many of the wrong things. But the term, as it is applied here, is used simply in the dictionary sense: it is intended to enforce the idea that managing agencies cannot write policy, or administer a program, or bring about a revitalization of management of anything that they do not actually foster, sustain, and support. We do not mean that Government should be an advocate of a special interest. We do not mean that Government should adopt a spirit of advocacy guided by the principle that information technology can be used to improve management.

In general, the current condition of the Government will only improve when there are major changes in attitude regarding information technology. A systematic and integrated effort will be required to affect needed change. This effort will require a commitment enunciated by the President. Our greatest concern now is that we get such a statement of commitment based on a recognition that the technology has achieved the required level of maturity and cost benefit.

It is because of this concern that the recommendation (stated in one of the earlier drafts, but later pulled back) for the creation of a "Special Assistant" was generated. The recommendation was an effort to make clear to the President the level of importance we attached to this problem. As it turned out, however, the idea of a special assistant did not receive a sufficient amount of support.

There are very few structural recommendations included in the entire report. Those that are present are viewed as crucial to effecting and maintaining possible changes. As the study has gone on and as actions have been taken, a number of changes have already occurred. As Wally Anderson indicated this morning, the DPA threshold at GSA is now \$300,000. The change in the technology suggests that one currently can buy substantial and significant systems under DPA. I do not view this as a major problem, but as a major opportunity (which may nonetheless warrant caution). Perhaps this change will allow us to begin operating on a cost basis at a different point on the overall cost curve.

This development, of course, introduces some additional factors besides that level of progress, the changes that have been effected in GSA, and the number of policies that are being drafted in OMB. One of the potential dangers is that someone will decide that the study has had its effect and that the only action to take is simply to allow the changes to take their course. I am convinced that that is not enough. I am convinced that there has been a spurt of activity and that the right direction has been indicated.

In order to sustain activity in the right direction, a number of basic structural changes must be made--particularly within OMB. One of these structural changes has to do with the establishment of an Executive Associate Director level of responsibility in information technology. We have asked

that the person who would take over that position in the OMB be agreeable to the idea of operating as a peer in a relationship with central players in the GSA, ADIS, and the Department of Commerce. One of the serious problems in leadership is that there does not appear to be interpersonal coalescence of purpose and activity across these agencies. We consider it important to establish a person at the right level, one who is recruited on the right basis, to bring off the kind of program that is called for here.

I am not going to attempt to go through the recommendations in detail, but will briefly comment on each of them. My comments are included in Recommendation One where it is stated that the Federal Government needs to (1) take action that will establish the importance of information technology, (2) provide tools for its management, and (3) set national and Federal goals for its productive use. We feel that change within OMB is important. There must be a change in each of the cabinet agencies establishing an "information resource manager" to work with and to form another level of peer group in the framework of a National Council for Information Technology, Policy, Plans and Programs.

One of the problems--for which such a Council might provide a remedy--is that, in the current situation, program agencies do not have a well-formed avenue for grief. If they complain to OMB, it never goes any farther--one way or the other. The real grief fails to get expressed. If they complain to GSA, they get the same result. To be effective, then, this Council needs to be constituted as a body of peers able to understand and deal with problems across agencies.

Most of the councils we see appear to be lobby points for the vested interests of the various agencies. One way to avoid this is to have a mechanism by which members are chosen with the approval of the council itself. This proposal has been interpreted as challenging the authority of cabinet agency directors. However, the important thing to realize is that a council or a committee rarely functions as an entity until it has some control over its own membership. Otherwise, you continue to have turf battles. This would be the extent of the structural changes we would propose.

The Second Recommendation states that the Federal Government needs to improve and expand its use of modern information technology to increase and enhance the level and quality of governmental service delivered while reducing cost. In this area, we would emphasize that while we talk about reducing costs through the use of the information technology, it must be recognized that this has to be done on the basis of an investment payoff. It can possibly be done by reallocation of priorities, rather than by expanding budgets; it should be undertaken with the idea that the cost of the information technology may rise when based on an investment. The value of any expansion of technology will have to be determined within the framework of the payoffs resulting from improved service and the like.

In Recommendation Three, we state that the Office of Management and Budget needs to establish a policy requiring that the cost of data processing be charged back to the using-agency in program-related terms. I could not help but think, when we were talking about the issue of post-audit this morning, that the mechanism called "zero base budgeting" provides an adequate and excellent basis for doing this on an annual review, provided there is an adequate performance tracked back to the budget package. The fundamental flaw in the current implementation in the area is that zero base budgeting has been approached more as a budgeting process than as a management tool. Until performance reporting is tied to the budget package and until the next budget package is a function of how well the previous one is satisfied, one does not get the kind of program audit that is needed in order to justify the funds expended. The recommendation is intended to set up a structure for a program that would recognize the strength of something that is already in place. Whether liked or not, it provides a basic mechanism for management.

The Fourth Recommendation is that the Federal Government set as an objective the removal from service of all information technology components which have outlived their cost-effective lives. This necessitates the development of some guidelines regarding cost-effectiveness.

I have to use my own analogy here. A lot of people say that just because a computer is old does not mean that it is not a good computer. That is true. I can understand that concept too. I have a 1966 GMC truck that is rusty, black and white, and has 16-inch wheels on it. I paid \$400 for it and have driven it over 10,000 miles. I drive it to work and back and it does a very good job. That is cost-effective utilization of an existing resource; capital investment, savings, operating costs--nothing would pay for the benefit that I get out of it. However, that utilization comes at a certain risk. I can use the truck only so long as I drive on dry days, maintain five car lengths between me and anybody else, and manage not to have any surprises; and as long as I do not visit my neighbors and park it in front of their new houses and do not drive it to see consulting contacts, etc. Those are the conditions under which I can profitably use that truck.

The issue of whether or not the Government's program equipment is obsolete or not is, I think, not what we are dealing with. Rather, we are dealing with issues of obsolescence and, really, with the trends and implications that go with it. The further implication of the trends is clearly underscored by actions that took place this year when the GSA established an "elephant burial ground." That is what I call it. It is a warehouse where you move computers that are out of production. The idea for warehousing them is that you can salvage parts from them so that you can continue to use those that are still in operation. But even in a university laboratory, I cannot afford that kind of approach to operation, for in the framework of what the technology provides today, it costs me more money to salvage an old piece of equipment than it does to go out and buy a functionally equivalent unit. The technology provides new approaches to questions of reuse and obsolescence.

Even though the concept of reuse appears to be excellent, it has been horribly abused. An example of this is the fact that once a National Guard organization has requested a computer and justified it--through the expensive process of its justification--the Department of Defense will ship them a 1401. It costs more to package a 1401 for shipment than it does to buy a replacement piece of equipment. It costs more to provide the power and the air conditioning than it does to provide the replacement part. This is the way in which institutionalized decisions break down or become a problem for the Government. Once you have established the principle of reuse, if you do not review it in the framework of management responsibility and cost-effectiveness, reuse becomes an objective in itself--an extremely expensive one. This is the basis for the recommendation.

Recommendation Five has to do with the Federal Government's need to significantly alter its process for acquiring information technology resources. Increased emphasis should be placed on the planning needs, definition, and justification phases of acquisition. In this sense, we salute the spirit and the direction of A-109. We recognize that, based on recent guidelines associated with A-109, it is applicable in the information technology and compatible with the objectives and purposes of Public Law 89-306. Further, it seems that GSA is having much difficulty administering a number of pilot projects in the A-109 area.

Some work does need to be done in the area of guidelines, classifications, and so forth. The spirit and direction of it, as a management planning process is, I think, acknowledged and valid. We will carry that acknowledgement further by saying we wish that all information technology procurement could be conducted under a uniform Federal procurement-type policy. That is one of the virtues of A-109. It applies across the board to major systems whether they are computer systems or aircraft carriers.

We feel that it is important that information technology not be singled out for special treatment. We would like to see the spirit and direction of the Federal Acquisition Act of 1977 carried forward and the technology procured under those constraints as a normal part of the responsibility of program and mission managers. In lieu of that, we go through a set of recommendations regarding the current situation in an attempt to provide some guidelines for implementing the current system.

Recommendation Six states that the Federal Government needs to (1) upgrade the training and career development required for functional managers, (2) reclassify personnel skilled in management or use of information technology, and (3) establish appropriate career paths for such purposes. It seems, on the surface, that civil service reform provides most of the mechanism we call for in the recommendation--except for the possibility of certain classifications within the technology itself. In this area we criticize the Defense Department and point out some things that they should look at.

Recommendation Seven states that program agencies (1) need to be strengthened to meet the general requirements for managerial and technical expertise in information technology and (2) must have prompt access to resources which can help them solve their problems. Under this recommendation, there is another minor structural factor. It is the responsibility of the Department of Commerce to provide the required assistance. We call for the establishment of special assistance centers to include both managerial and technical support. We feel that managerial assistance is badly needed in many areas.

Recommendation Eight states that the Federal Government needs to institute a research and development program in information technology to meet the needs of the nondefense sector. We hope that as a result of this recommendation we will establish an approach that would provide a mechanism by means of which the Government can quickly come abreast of the set of research products that exist in the private sector for a particular area. We propose that the recommended program be established rather than another competitive research organization.

Government has problems in the information technology that the private sector is not going to be responsive to because so much of private research is market driven. Some of the problem areas that the Government has to deal with--particularly in areas of privacy, security, identification, and so forth--stem from the fact that basically the Government is the principal market for this information. That may not be enough to sustain the right activities in the private sector, so we attempt to address that problem.

The Ninth Recommendation, the final one, states that the Federal Government needs to revitalize its efforts to establish and maintain a standard program for information technology in order to support the economic purchase of equipment and the economic and effective operation of computer resources.

That is basically a profile of the findings, conclusions, and recommendations of the report. The report includes summaries from all of the various team reports. It also includes what I have chosen to call an implementation plan--though it is not in itself an agenda of actions; rather it is a proposal to establish a peer-group planning body to establish procedures and recommend actions to implement the total set of recommendations. In addition, the report includes an acknowledgement of a strong minority position urging the creation of a special assistant to the President--a proposal which is not a recommendation agreed to by the majority.

Staats: What was the main point in the minority report?

Jensen: The variety of points that are made in the minority report have to do with the dilemma that exists concerning the failure of the central agencies to accept responsibility. The need to bring about changes, it was felt, justified presidential emphasis on this level. Without that kind of emphasis, the OMB, GSA, and Department of Commerce are not going to change. That is the substantive position of the minority.

Eirich: A couple of weeks ago, or maybe it was longer than that, I listened to a talk by Mr. Henry Geller who said the study was completed and about to go to the President. He was not talking about this study, was he? Is there a separate study?

Jensen: I suspect it is a separate study.

Eirich: What was interesting, Mr. Geller mentioned that they were going to try to come up with an overall U.S. information policy. However, they found that they could not come up with overall policy but rather with seven different policies. One of these policies dealt with the information technology. I was wondering if you are going to find yourself in competition? He did not give any details on what they found. He said he just could not at that time.

Jensen: This is one of the changes that basically concerned us in the course of the study. National Telecommunications and Information Administration (NTIA) was formed about the time that we were finishing up the study. One of the things that concerned us about it was that the Executive Order that established NTIA was vague with respect to information technology.

Heller: I am a little confused as to where you come out on the Brooks bill. I am not quite sure whether you are walking a political line here or what you are doing. You gave me the impression that maybe it is okay, and then maybe it is not okay.

Jensen: I hope that I took a very strong position that the Brooks bill is a fine piece of legislation.

Heller: For its time, or for now?

Jensen: For any time.

Heller: You say as a legal framework?

Jensen: Yes. As a framework. Its implementation has left much to be desired. Some changes, therefore, clearly need to be made.

Heller: How do you revise that since it seems to me that some of the poor administration that is going on has been fostered by those who hide behind the shield of the Brooks bill. How do you fit that?

Jensen: Here again is where we feel that the focus and the attention has to come from the President. Leadership has to be provided.

Heller: Is that what you mean by your one recommendation in here about the intrusion of the legislature into the executive branch other than through the General Accounting Office?

Jensen: Well, one of the things that we would emphasize there is that we want to recognize that oversight is a legitimate function of the legislature. This fact probably is not appropriately worded in the draft, but there is clearly evidence that oversight has pre-empted the decisionmaking process.

Staats: I would like to follow up on John Heller's question and get your reaction to this point. At the time the Brooks bill was being considered, there was very heavy emphasis on computer lease versus purchase and on computer sharing. At the time, of course, they were very, very expensive and everybody could understand that. Now we have moved on to the technology of smaller and less expensive units as far as the hardware is concerned. I wonder to what extent that should affect our thinking as to the role of GSA in the procurement field. I am thinking about the procurement only.

Jensen: I am not a procurement expert, but my reaction is that one of the things that happened to the Government about 1965 was that a great truth was discovered. That great truth has to do with economy of scale. This basically says that big computers are great. But Pete Jensen's corollary of Grosch's Law (quoted earlier today) states that when cost per unit for computing is a function of the size of the computer, there is a decrease in function. This was shown to be imperative about 1965 with the emergence of high-order operating systems, multi-programming concepts, and so forth. The opportunity seemed to be supportive of the larger systems in providing the lower unit of cost. This is predicated on the notion that one will use all the material in the box all the time. With the impact of an electronic packaging technology, we have not had a lot of revolution in computing. The packaging technology has not repealed the economy-of-scale concept. It has, however, brought about worthwhile changes in terms of the nature of the economy scale which appear in large systems based on the kind of volume which GAO may have.

This is the fact that is currently being ignored. This is the kind of fact that increases the cost of "preventing sin" and continues the emphasis on centralization as if the centralization

Heller: How do you revise that since it seems to me that some of the poor administration that is going on has been fostered by those who hide behind the shield of the Brooks bill. How do you fit that?

Jensen: Here again is where we feel that the focus and the attention has to come from the President. Leadership has to be provided.

Heller: Is that what you mean by your one recommendation in here about the intrusion of the legislature into the executive branch other than through the General Accounting Office?

Jensen: Well, one of the things that we would emphasize there is that we want to recognize that oversight is a legitimate function of the legislature. This fact probably is not appropriately worded in the draft, but there is clearly evidence that oversight has pre-empted the decisionmaking process.

Staats: I would like to follow up on John Heller's question and get your reaction to this point. At the time the Brooks bill was being considered, there was very heavy emphasis on computer lease versus purchase and on computer sharing. At the time, of course, they were very, very expensive and everybody could understand that. Now we have moved on to the technology of smaller and less expensive units as far as the hardware is concerned. I wonder to what extent that should affect our thinking as to the role of GSA in the procurement field. I am thinking about the procurement only.

Jensen: I am not a procurement expert, but my reaction is that one of the things that happened to the Government about 1965 was that a great truth was discovered. That great truth has to do with economy of scale. This basically says that big computers are great. But Pete Jensen's corollary of Grosch's Law (quoted earlier today) states that when cost per unit for computing is a function of the size of the computer, there is a decrease in function. This was shown to be imperative about 1965 with the emergence of high-order operating systems, multi-programming concepts, and so forth. The opportunity seemed to be supportive of the larger systems in providing the lower unit of cost. This is predicated on the notion that one will use all the material in the box all the time. With the impact of an electronic packaging technology, we have not had a lot of revolution in computing. The packaging technology has not repealed the economy-of-scale concept. It has, however, brought about worthwhile changes in terms of the nature of the economy scale which appear in large systems based on the kind of volume which GAO may have.

This is the fact that is currently being ignored. This is the kind of fact that increases the cost of "preventing sin" and continues the emphasis on centralization as if the centralization

10-11-65  
D. J. K. F. E.

were an end rather than a means. As Jack Jones and other people will point out, you (1) centralize when it pays out, (2) decentralize when it pays out, and (3) mix the two in order to give yourself the best profit course. This is the element that is currently lacking in the implementation because of the urgencies that came through the House Government Operations Committee. There is a lack of recognition of the impact of this kind of an opinion.

The other issue is that part of the cost of preventing sin has to do with the cost of competition. Often one sees a situation in Government where competition is exercised for competition's sake. For 20 years plus, I have been advocating competitive procurement—but only where competitive procurement has a payoff. My current guideline in my own institution is that if you are not likely to save \$100,000 through competitive procurement methods, do not do it, because it costs you that much to go through the procedures.

Staats: Do you want to address yourself to the question that Wally Anderson was referring to this morning on the issue we have between the Government Operations Committee and the Appropriations Committee dealing with what you should include in that cost analysis?

Jensen: I can give you my personal opinion. I think that procurement of computer systems that does not include the conversion costs is a fallacy.

Staats: You think it should be included?

Jensen: It has to be. We cannot evaluate the investment that GAO is going to make without some consideration of conversion. After all, if it's a business application and you are going to make an investment for profit, you have to consider conversion. To give you an example of what we do at Georgia Tech—we had a strange experience with UNIVAC 1108. We decided we need an 1110. We were running out of horsepower, and we wanted to do an incremental procurement. We were forced by the State to do a competitive procurement. Since we were going to do a procurement, we decided to do it right.

We put together a very comprehensive program including a benchmark, evaluation, and so forth. We included in that the cost of a whole operation. In fact, we required the winning vendor to take the 1108 as a trade-in. This caused some people to not want to bid. One vendor suggested that the RFP was glued in or wired into UNIVAC. We said no, we've got an 1108 and we just want the cash value of its worth. We'll find the third party to buy it if

you will bid. IBM chose not to bid anyway; Honeywell, for various reasons, did not. We came up with the competition between Control Data and UNIVAC. It turned out that for our benchmark—cost of converting included and accepting the trade-in of the 1108 and so forth—Control Data's bid was much lower than UNIVAC's.

Staats: There is another point here, to which you might have some reaction. What we have been thinking about, without arriving at a firm conclusion yet, would be looked at as a two-step process. The first step would be to make a judgment as to whether or not the upgrading is worthwhile—i.e., cost effective. In that case, in the first step you would include the cost of conversion. In other words, you stick with what you have, or you go to something more advanced. But, once you have made that cost-effectiveness analysis, you should exclude the conversion costs in the interest of putting all bidders on the same basis, and on the basis of standard language. I guess Don and Wally could state this better than I can, but we have been thinking about that in a kind of two-stage process. This represents, I think, the difference between the two committees and their approach to this area. Until we have done more study on it, we are in the middle of the subject.

Jensen: There are more differences than that between the two committees; I do not know what causes the differences. The issue of conversion is being used as a mechanism for saying that it precludes competition. My reaction is that every functional requirement statement precludes some competition. As a functional requirement, there has to be someone who cannot do it. If the business of procurement is to be carried on in the best interest of the Government, it appears to me that it must be carried on in the framework of a fully competitive process in which all the cost factors are considered. This is my personal opinion.

There is still another issue. I think it states that the technology here is in the framework of what is called the soft architecture computer. It provides the opportunity to do what I think the House Appropriations Committee calls an architecturally specific procurement. This would mean that there are people who were producing systems that acted like an IBM 370/138 for substantially less money. There are a number of such vendors that provide that kind of system. The reason for competitive procurement would be that it simply replaces the function at a reduced total cost.

This is predicated on a very important assumption. That assumption is that the agency is doing what it should be doing, the way it should be doing it. All they need is a new level of horsepower that can be provided through the technology.

The procurement process is being used for purposes other than that. The process is being used to affect management in the program mission agencies to bring about different kinds of planning. In such cases, the procurement leads to a situation in which an agency, which has a failure in its current process, spends 3 years trying to obtain a piece of equipment that it really needs.

Staats: Wally, where would the Brooks staff disagree with what he just indicated here?

Anderson: The Brooks staff would disagree on the software part. If the software were in machine-specific or assembler language, they would not allow that conversion cost to be used as an evaluation factor. They would agree if the programs were in COBOL and they required change from UNIVAC COBOL to Control Data COBOL. They call that "out-of-pocket" to indicate that it is necessary, but too small. It may not be small though; it may be large. We find that there are many other factors of conversion including training, site preparation, and many methods of operation that have to be changed. We are attempting to document all factors.

Our conversion report and standards report, among other things, relates to this issue. With these reports, we are trying to minimize the size of the conversion to make it less of a swing factor in the competition. The Appropriations Committee has aided our efforts. They are calling for life cycle costs. Now, when you include in any procurement conversions costs beyond the raw equipment itself--such as all the life cycle costs--conversion becomes a smaller factor. Conversion might be just 30 percent if you consider only equipment prices in conversion; if you put other factors in, such as life cycle costs, conversion becomes a smaller factor--say 10 percent.

Staats: That is because you amortize it over the expected life of the equipment.

Anderson: Right. The conversion then is a smaller factor and becomes less of a determinant in the procurement. I think you (Professor Jensen) did something like this in your procurement at GeorgiaTech and it was not a swing factor. You proved it!

Jensen: The kind of thing that one must take into consideration, I think, in life cycle costs of the system is the fact that one tends to be cautious about long-term investment in a system. Basically, one should build into the system some aspect of instrumental upgrading as a part of the overall process.

Anderson: They all agree to that.

Eirich: Would you agree that if you compute life cycle costs which you convert to standardized higher-level language, your maintenance and preparation of new software for that life cycle will be lower than if you have a nonstandard language?

Jensen: I think that one of the great virtues of COBOL, for instance, is that it has provided that kind of opportunity. To say that, in general, everything should be COBOL is something I do not accept.

Eirich: No. I was thinking of any ANSI statement.

Jensen: If there were adequate standards. There is another problem here. This is not going to preclude conversion because even with it, one has a family of standard languages. All of the vendors are going to have enrichments on the standard. There is no adequate enforcement mechanism to ensure that programmers are going to use the standard. They use the standard plus the enrichment. As a consequence, one ends up with nonstandard programs--all of them including the enrichments. I worked for a year trying to find the set of ANS FORTRAN programs in my organization. I never did find it. The only ones I found were in the Navy Department, and the reason I found those was the Navy was using them to test the FORTRAN compilers. That is the only reason they were standard.

Q: How did you feel about the question (after coming up with your conversion costs) of allocating between new development costs and ongoing operating costs? And how did you feel when you came up with that conversion cost element to evaluate in GAO's procurement?

Jensen: We have probably a more complex problem than most people because we have approximately 9,000 programmers on campus. All the researchers or administrative organizations, etc., are doing all their own work. We have a computer facility in which little applications programming is done within the computer center.

As a consequence, we have a serious problem. Part of the benchmark we put together included programs from every place we could get them on the campus--all the simulation languages; all the special languages that people had. One of the requirements--and the measure of the benchmark--was that the vendors had to run as many of those programs as they could to give us the measure of what we were going to confront in development costs downstream. So we came up with a situation that was favorable to us anyway. Control Data seemed to have little difficulty converting to all the problems for some reason.

Staats: Is there anything that you have written that bears directly on this question of what we were talking about a few minutes ago on the extent to which you included conversion costs?

Jensen: In the framework of the Reorganization Project?

Staats: Well, either that or otherwise?

Jensen: Not within the framework of the Reorganization Project.

Anderson: Thank you.

ADP TECHNIQUES HAVE SUBSTANTIALLY  
IMPROVED ADP AUDIT CAPABILITY  
AT THE GAO

by

Michael Zimmerman  
Assistant Director  
Human Resources Division  
U.S. General Accounting Office

February 13, 1979

Introduction of Mike Zimmerman by Don Scantlebury

We have covered a lot of territory today, some of it futuristic and some it pretty much down to earth. It all adds up to changes which are affecting the way Government does business. This is affecting us here at GAO as well, and our response will be crucial to the type of role we will play in the future.

Let's look at the response by one audit group in HRD. Mike Zimmerman, the Assistant Director at the Social Security Administration, is going to take about ten minutes to tell you what happened to him and his group when he was forced to face up to the computer. After his talk, I'll have some general comments on computer auditing, and we can have the general discussion Mr. Staats mentioned when he opened the program today.

Mike Zimmerman - Summarized

- I. ADP technology used by SSA has had a major impact on the way we evaluate SSA's programs.
  - A. All SSA programs use very large, complex computer systems to accomplish their missions
  - B. Had avoided looking at the ADP systems until the horrors of the Supplemental Security Income program's overpayments hit the papers and we received Senator Birch Bayh's request.
  - C. Now needed to audit the program in its entirety--including the ADP system.
  - D. Regular auditors did not know how to talk "computerese" much less understand it and be able to audit it.
  - E. Had to get people that were auditors first, but had additive skills which allowed them to audit in the ADP environment.
  - F. Put self on line with HRD management--requested assistance from FGMSD/TAG-DP's computer auditors--had to accept full responsibility if they couldn't provide good report products.
- II. Began their involvement with a reliability assessment of the SSI program.
  - A. Used the reliability assessment to identify potential control weaknesses in the SSI program--note the word "program" because that is exactly what they audited (not just the SSI computer system), but the entire program--from the initial recipient interview through the manual and automated procedures until the recipient gets his final award/denial and all the steps in between.
  - B. Many control weaknesses were identified--both manual and automated.
  - C. Several jobs were quickly spun-off of this reliability assessment, including:

1. "Review of Difficulties Encountered by SSA in Obtaining Pension Data from other Federal Agencies for Purposes of Avoiding SSI Overpayments"
  - Took 2 percent sample of 4.2 million SSI recipients (84,000 + records).
  - Matched these records to VA and RRB computerized master pension files (over 15 million records were processed).
  - After verifying matches, recomputed SSI benefits, substituting the correct VA and RRB data, using SSA's own computation program.
  - Identified over \$56 million in overpayments and \$4 million in underpayments.
  - SSA took immediate action and now estimates savings in excess of \$100 million.
2. Other matches, including:
  - Workmen's Compensation
  - Black Lung Benefits
  - Student Benefits
3. "Review of Internal Controls and Performance of the SSI System"
  - Review begun to evaluate the entire SSI system.
  - Evaluated the manual processing procedures in SSA field offices (visited 30+ offices throughout country).
  - Evaluated the applications system by testing the computer programs.
    - Created a new and innovative approach.
    - GAO has received a lot of favorable publicity from this new technique.

--Evaluated the controls over SSA's telecommunications system and central computer facility.

--To date, four reports have been issued under this job code, and two more are in draft, including the final report to the Congress which identifies \$25 million in erroneous payments caused by control weaknesses in the SSI program.

--Additionally, findings, conclusions and recommendations have been added to two other reports as a result of work done on this review.

III. Other significant activities at SSA which required ADP knowledge include:

A. "Review of Unresolved Earnings Records in the Social Security Program"

1. Took sample of 866,000 records from the 173 million records on the wage earners suspense file.
2. Developed a new technique that allowed us to post \$4.4 billion (out of the \$35.7 billion suspense) to 6.6 million recipients' records.
3. SSA is presently incorporating our technique into their on-going posting process.

B. "Review of President Carter's Welfare Reform Proposal--The Better Jobs and Income Bill"

1. Used computer auditors to comment on the ADP aspects of the proposal, including
  - a. the technical feasibility of the computer system required by the proposal; and
  - b. the security/privacy implications of the proposal as they related to the computer system, etc.

C. "Review of Major ADP System Development Plans at the Social Security Administration"

1. Congressman Jack Brooks' request.
2. Congressman Brooks has stopped all major ADP procurements at SSA, pending GAO review.
3. Computer auditors used to evaluate ADP aspects of procurements, and new application system proposals, and also functional aspects of all SSA programs.

CLOSING REMARKS

by

Donald L. Scantlebury  
Director  
Financial and General Management Studies Division  
U.S. General Accounting Office

February 13, 1979

Don Scantlebury

I think Mike Zimmerman has made it clear how we can use computers to help us do our work, with, I might add, technical assistance from the FGMSD-TAG Group.

A couple of years ago we assessed other agencies' computer audit capability--there is no question that right now GAO's capability is considerably ahead of any other government agency. However, the other agencies are beginning to take more interest and, in the future, their auditors will be doing much more computer auditing.

Vital to the development of this capability, of course, is a successful training program. Our training program, which I feel is a very effective one, began with a study that Clerio Pin and Ken Pollock made in 1971. Their work led to the Wharton Course and various other training courses.

Let me give you an idea of the various courses GAO people have taken. About 250 people have completed the Wharton Course. Around 1,650 people have taken our Base Level Training Course, which deals with basic knowledge that every GAO auditor ought to have. The Beginning Time Sharing Course has been offered to 80 people; the Advance Time Sharing Course to 40 people. In addition, 60 people have completed the Reliability Assessment Training Course, and 107 people have taken the Data Retrieval Course.

So, as you can see, we have done quite a lot of training recently.

We have also issued an addition to the yellow book which sets forth the standards for DP audits. I have an advance copy of it right here. You all have had a chance to review it and send us your comments, which we have considered. The addition is at the printers now and will be issued shortly.

Before we close our presentation, I would like to call a serious problem to your attention. It is a problem affecting the whole agency and is one that we will be discussing in the Directors' meeting very soon. That problem is what is happening to our ADP capability.

Our division program plan contains a line of effort (0108) entitled "How Effectively Do Computer Systems Aid

Managers and Users in Carrying Out Mission Requirements and Support Functions?" This particular line of effort should be useful in many of the other divisions, and I hope you will do some work under this issue area in the next year or two.

To help along that line, we accumulated information on agency plans for major ADP telecommunications acquisitions for the next 5 years. We have sorted the information by division area of responsibility, and Ken Pollock will give each division representative a list.

As I mentioned earlier, we have been doing a lot of work for Congressman Brooks' Government Operations Committee. We were asked to look at potential procurements, many of which the Committee felt, for good reasons, were not warranted. We expect these requests to continue during this next year, and will therefore expect to need a number of procurement evaluations. We, in FGMS, will be working with many of the other divisions during the coming year on such cases.

That concludes our presentation for today. I want to thank all the other divisions for their contributions. The material on display around the room was contributed by all the divisions and it shows some of the good things that we, as an agency, have done in the computer area.

As we close, Mr. Staats has a few remarks for you.

FINAL STATEMENT

by

Elmer B. Staats  
Comptroller General  
of The United States

February 13, 1979

Mr. Staats

Closing Statement

I think this program has worked out extremely well, and I want to thank you, Don Scantlebury and Wally Anderson, and all who contributed in putting the program together.

One of the several things I had hoped to achieve during my term here and something I talked with Mose Morse about at length was that GAO should be in the forefront in the automatic data processing area--we should be second to none anywhere in the Government or in the country.

I think that what we have seen since 1966 is a revolution. I used that term this morning and I do not think that it is too strong a word to use both in terms of what has happened in the technology here at GAO and in terms of investment. I believe that the Federal Government bought its first computer in 1951, which is really not that long ago. If you look at how computers have changed between 1951 and today, I think it is appropriate to call their development a revolution.

I am concerned about the point that you and others have made of how we are going to retain the capability that we have developed. I do not know the answer, but I think we are going to have to find it.

There is one school of thought on the subject which would put all GAO computer work in one division. For obvious reasons I do not think that is the solution. We must build computer capability into every operating division within GAO. That is not to say that we don't need our current expertise, but we must have not only what FGMS can bring to the work of the divisions in terms of TAG work, but each division must have its own computer capability. I think that all of us recognize that. What we must do is retain enough ADP expertise in the divisions and in the regional offices for division directors or regional managers to use. The divisions cannot rely completely on TAG to provide the assistance.

We will be addressing this problem here, particularly with Felix's help. In the meantime, however, if you have any ideas or suggestions on this point in your division directors' meetings, I hope you will put them on your agenda and see what options you can come up with for dealing with this problem.

Many thanks to you, Don, and your staff for your help in a successful presentation.

PUBLICATIONS OF SELECTED ARTICLES (By FGMSD/ADP)

The first page in this section is a reproduction of the cover for the "Selected Articles on ADP/Auditing" (334 pages) assembled and printed in conjunction with this briefing. Copies of the entire publication were distributed to division and office attendees and to the regions.

DISPLAY CHARTS (By FGMSD, FPCD, EMD, CD, GGD, LCD, PSAD,  
OCG, OL)

The following pages contain reproductions of the 30" x 40" charts voluntarily designed by various GAO divisions, prepared by the Illustrating Services Office, and displayed on the ledges around the Comptroller General's briefing room during this all day session. The charts depict how knowledge of ADP and development of related techniques have substantially improved GAO's overall audit capability.

DEMONSTRATION (By FPCD)

The last picture shows a live demonstration of a computer application being conducted at break times in the briefing room. The demonstration showed how a computer connected terminal is used in the analysis of data and the documentation of results required by a typical audit assignment.

Selected Articles

# Auditing

# ADP

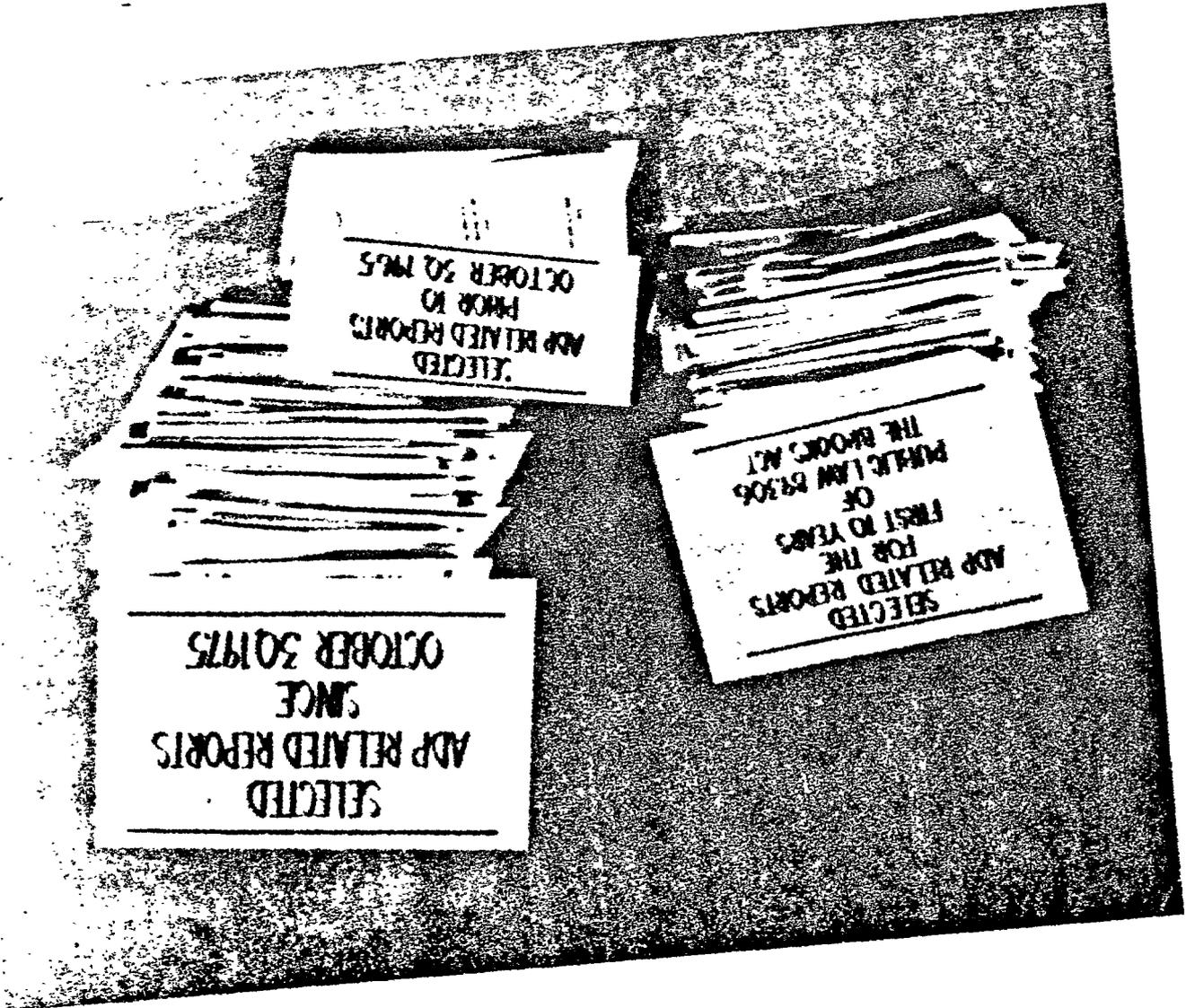
# ADP



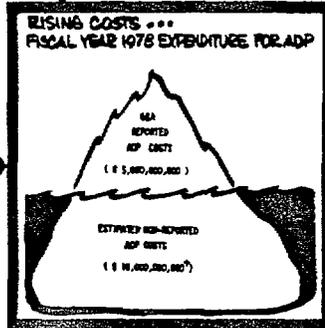
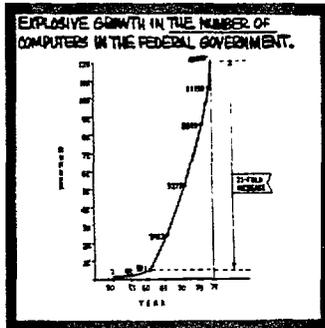
EXECUTIVE  
ADP BRIEFING  
FEBRUARY 13, 1979

13.1

FGMSD-ADP



# GAO COMPREHENSIVE ADP EDUCATION PROGRAM (CODE 91311)



REALITY (COMPACTIFIED BY HEADLINES)

### COMPUTER WASTELAND USA

SRJ Fault Management  
DP Auditing Found in Poor Shape

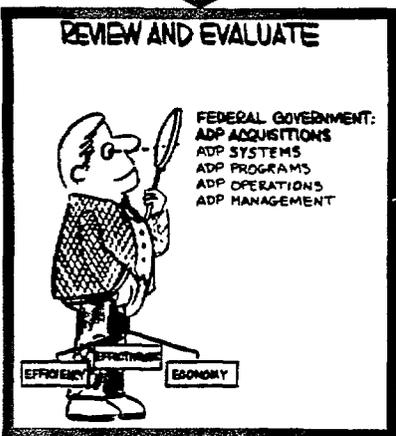
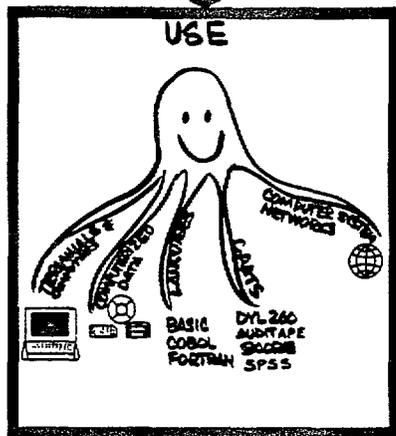
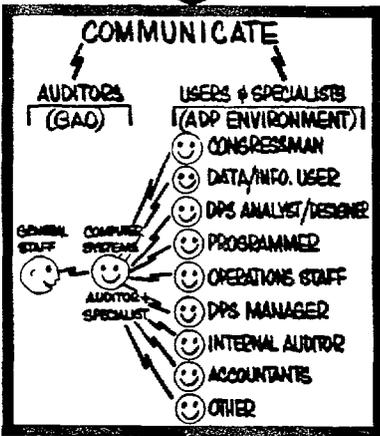
Computer Auditing In The Executive Departments. Not Enough Is Being Done

CG MEMORANDUM: SEPTEMBER 20, 1976  
"I HAVE COMMITTED THE OFFICE TO A STANDARD OF EXCELLENCE IN ADP CAPABILITY. I EXPECT ALL OFFICIALS & STAFF MEMBERS TO TAKE THE NECESSARY STEPS TO ACHIEVE THIS STANDARD."

CG MEMORANDUM: OCTOBER 1971  
DIRECTED ALL GAO UNITS TO:  
1. INTENSIFY AUDIT WORK INVOLVING ADP  
2. DEVELOP GREATER ADP AUDIT CAPABILITY  
3. PUT MORE EMPHASIS ON ADP TRAINING

BROAD OBJECTIVES ESTABLISHED BY FORMED  
**DEVELOP INTERNAL CAPABILITY TO:**

- COMMUNICATE EFFECTIVELY WITH USERS & SPECIALISTS IN THE ADP ENVIRONMENT.
- USE THE COMPUTER AS A TOOL IN PERFORMING REVIEWS.
- REVIEW THE MANAGEMENT OF ANY TYPE OR SIZE INFO INFORMATION SYSTEM OR PROGRAM GUARDED BY AUTOMATIC DATA PROCESSING.



BASE LEVEL ADP COURSE I (1900 STUDENTS)  
BASE LEVEL ADP COURSE II \*

(CAATS)  
BASIC TIME SHARING (80 STUDENTS)  
ADVANCED TIME SHARING (40 STUDENTS)  
AUDIT DATA RETRIEVAL (107 STUDENTS)

ADV. ADP CONCEPTS (MILITARY) 259 STUDENTS  
RELIABILITY ASSESSMENT (60 STUDENTS)  
COMPUTER PERFORMANCE EVAL. (82 STUDENT)  
AUDITING ADP DOCUMENTATION \*  
INTERNAL CONTROLS \*  
DATA BASE MANAGEMENT \*  
ADP PLANNING \*

**ADP AUDIT ASSIGNMENTS**

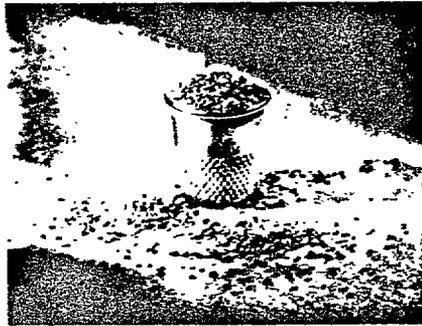
\* PLANNED

# ADP EDUCATION PROGRAM 5 YEAR PLAN (1979-1983) RESPONSIVE TO:

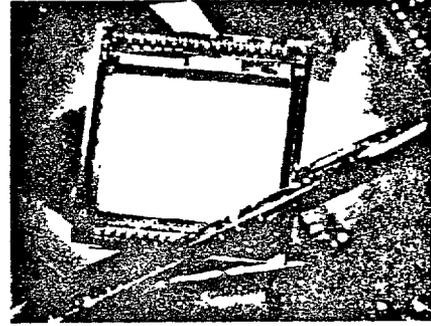
- \* CG DIRECTIVE
- \* ADP POLICY (CAM I CHAPTER 11)
- \* OMS "ADP TRAINING PROGRAM" POLICY MEMORANDUM
- \* CG "CLARIFICATION OF RESPONSIBILITIES FOR AUDIT WORK & TRAINING INVOLVING ADP" (SEPT. 20, 1976).
- \* CG "FURTHER CLARIFICATION OF RESPONSIBILITIES FOR AUDIT WORK INVOLVING ADP, B-115369" (FEB. 14, 1978).
- \* ADP ISSUE AREA LINES OF EFFORT (FGMSD-ADP)
- \* ADDITIONAL GAO AUDIT STANDARDS (AUDITING COMPUTER BASED SYSTEMS)
- \* PROFESSIONAL KNOWLEDGE & PERFORMANCE REQUIREMENTS AND STANDARDS.
- \* PRESIDENTIAL/CONGRESSIONAL CONCERN AND INTEREST
- \* GAO MISSION AND ADP AUDIT OBJECTIVES
- \* GAO PROFESSIONALISM, EXPERTISE, & LEADERSHIP
- \* INDIVIDUAL ASPIRATIONS FOR DEVELOPMENT & ADVANCEMENT



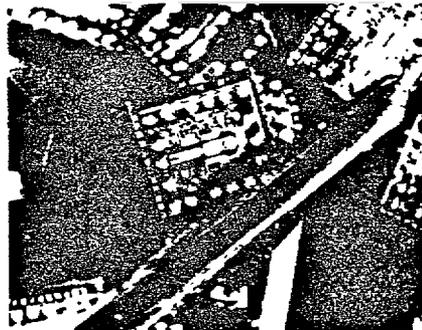
# COMPUTER COMPONENTS: PAST AND PRESENT



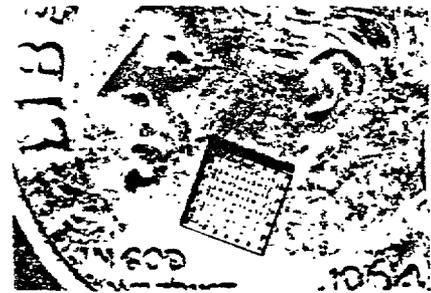
50,000 CHIP TRANSISTORS USED ON  
SOLID LOGIC TECHNOLOGY MODULES



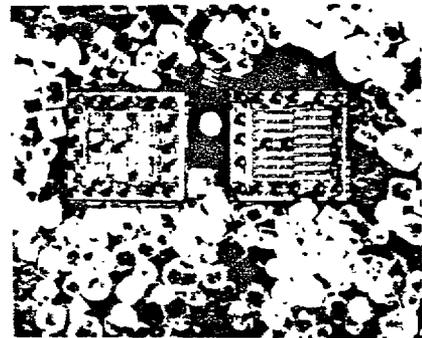
48,000 BIT READ ONLY STORAGE CHIP  
(HELD BY A NEEDLE)



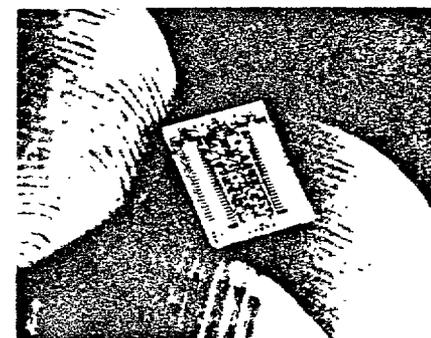
SILICON MONOLITHIC CHIP CONTAINING 25 LOGIC  
CIRCUITS



LOGIC CIRCUIT CHIP ON FACE OF DIME



HIGH-SPEED LOGIC (LEFT) + RANDOM ACCESS MEMORY (RIGHT)  
CHIPS SURROUNDED BY TABLE SALT PARTICLES

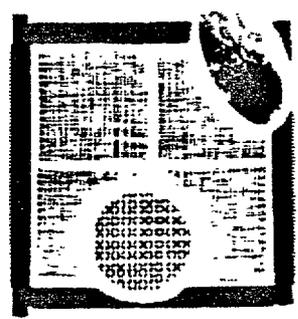


NEWEST MEMORY CHIP CAN  
HOLD UP TO 64,000 INDIVIDUAL PIECES  
OF INFORMATION (CIRCA 1979)

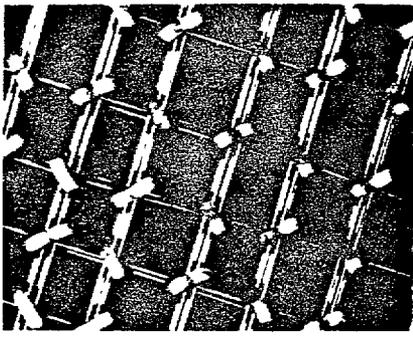
# COMPUTER COMPONENTS: PAST AND PRESENT



CHATHODE RAY TUBE STORAGE  
(MAIN MEMORY) (CIRCA 1953)



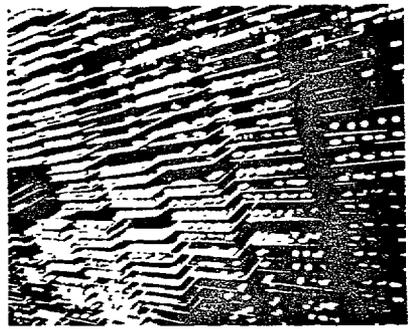
MAGNETIC CORE PLANES USED IN MAIN MEMORY  
(CIRCA 1955)



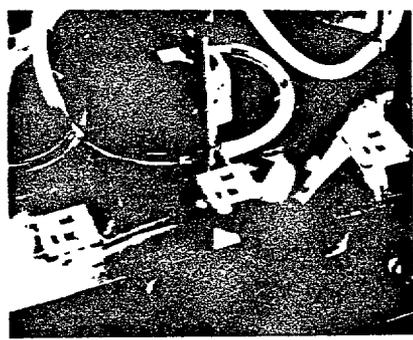
MAGNETIC CORE PLANES USED IN MAIN MEMORY  
(CIRCA 1964)



THREE GENERATIONS OF TECHNOLOGY  
VACUUM TUBES (CIRCA 1955) TRANSISTORS (CIRCA 1960) SOLID STATE (CIRCA 1964)

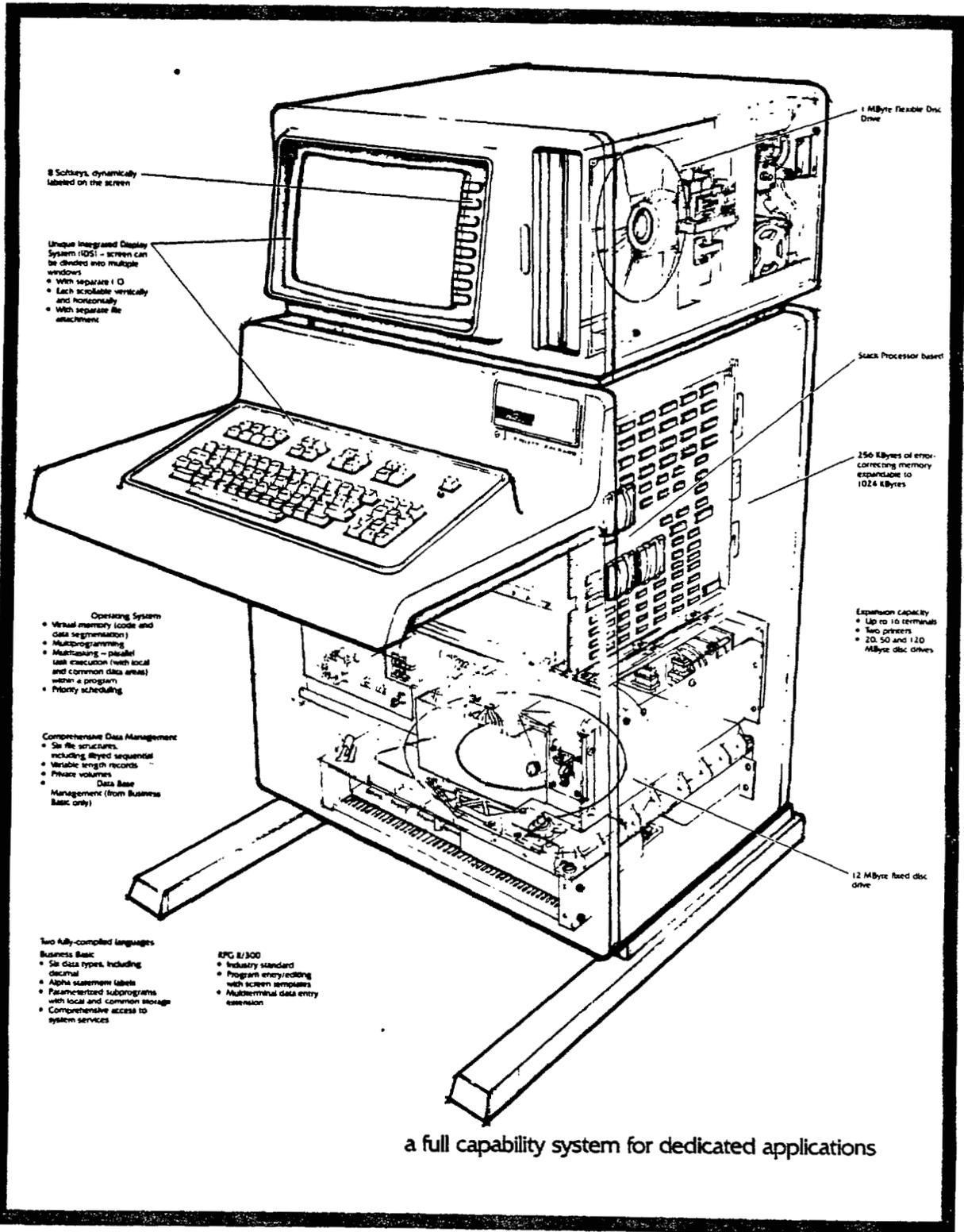


BANK OF PRINTED CIRCUITS CONTAINING  
TRANSISTORS (CIRCA 1960)



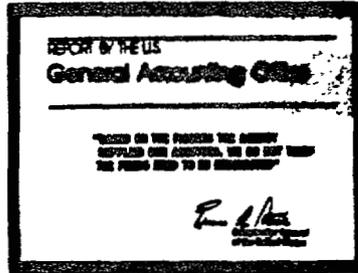
SOLID LOGIC TECHNOLOGY MANUFACTURING  
PROCESS  
(PLACING A TRANSISTOR AT A JUNCTION POINT)

# AN INTELLIGENT TERMINAL



# THE FINANCIAL GENERAL MANAGEMENT STUDIES DIVISION

## TECHNICAL ASSISTANCE GROUP-DATA PROCESSING COMPUTER AUDITING!... WHAT'S THAT?



JUST HOW CONFIDENT ARE WE THAT OUR FINDINGS ARE BASED ON RELIABLE DATA?

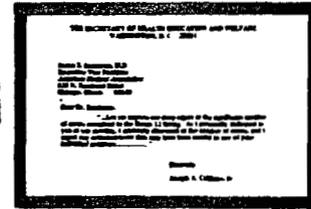
HERE'S AN EXAMPLE OF ONE EXECUTIVE AGENCY HEAD WHO FOUND HIMSELF OUT ON A LIMB!



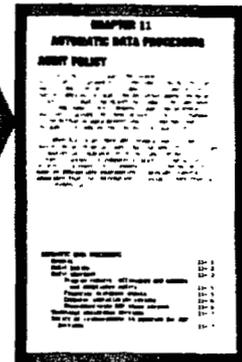
- \* HOW CAN YOU TELL IF THE DATA IS ACCURATE?
- \* WHY SHOULD YOU CARE?
- \* WILL IT INFLUENCE YOUR FINDINGS?

COMPUTER AUDITORS CAN TEST THE DATA AND THE SYSTEM THAT PRODUCES IT USING TOOLS AND TECHNIQUES DESIGNED FOR THAT PURPOSE.

**WHAT IS A COMPUTER AUDITOR?**  
HE/SHE IS FIRST AND FOREMOST AN EXPERIENCED GAO AUDITOR WHO HAS ACQUIRED ADDITIONAL TRAINING IN THE FIELD OF AUTOMATIC DATA PROCESSING (ADP) & IS CAPABLE OF APPLYING THIS NEW KNOWLEDGE TO AUDITING.



BY THE WAY.. ARE YOU FAMILIAR WITH GAO'S POLICY WITH REGARD TO USE OF COMPUTER PRODUCED INFORMATION?



 **LET US HELP YOU**  
**BEFORE BEGINNING YOUR**  
**NEXT AUDIT, VISIT THE**  
**OFFICE OF LIBRARIAN**  
**TO LEARN ABOUT OUR**  
**AUTOMATED BIBLIO-**  
**GRAPHIC SYSTEMS.**

- SCORPIO
- ERDA-RECON
- MEDLARS
- JURIS
- DIALOG
- ORBIT
- NEW YORK TIMES  
INFORMATION BANK
- OCLC



# **CLAIMS DIVISION..**

## **ADP EFFORTS**

### **INTERNAL EFFORTS**

**ACCOUNTS RECEIVABLE**

**MANAGEMENT REPORTS**

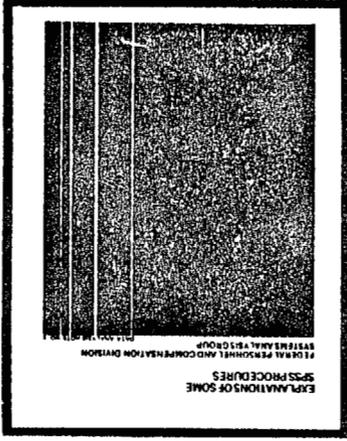
**CLAIMS LOCATOR SYSTEM - SHOWN AT RIGHT**



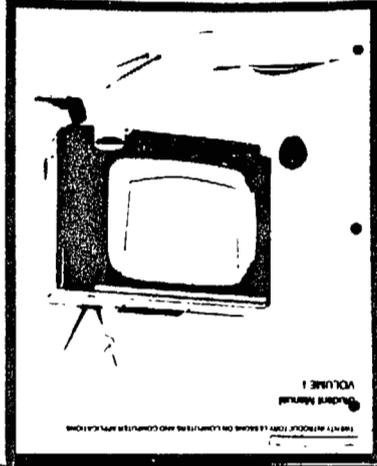
### **EXTERNAL EFFORTS**

**ASSISTANCE TO AGENCIES IN CLAIMS  
PROCESSING.**





**ADVANCED TRAINING COURSE**



**BASE LEVEL ADP COURSE**

OFFICE PROGRAMS AND PROCEDURES

FOR THE PERSONNEL AND COMPARATION DIVISION

PART I: OFFICE PROCEDURES

SECTION 1: GENERAL INFORMATION

SECTION 2: PERSONNEL PROCEDURES

SECTION 3: COMPARATION PROCEDURES

SECTION 4: MISCELLANEOUS PROCEDURES

SECTION 5: APPENDICES

SECTION 6: INDEX

SECTION 7: GLOSSARY

SECTION 8: REFERENCES

SECTION 9: CONTACT INFORMATION

SECTION 10: OTHER INFORMATION

SECTION 11: INDEX

SECTION 12: GLOSSARY

SECTION 13: REFERENCES

SECTION 14: CONTACT INFORMATION

SECTION 15: OTHER INFORMATION

**MANAGEMENT DATA SYSTEM (MDS)**

**OTHER ADP APPLICATIONS**

INVENTORY OF FPCD MACHINERY

SECTION 1: GENERAL INFORMATION

SECTION 2: PERSONNEL PROCEDURES

SECTION 3: COMPARATION PROCEDURES

SECTION 4: MISCELLANEOUS PROCEDURES

SECTION 5: APPENDICES

SECTION 6: INDEX

SECTION 7: GLOSSARY

SECTION 8: REFERENCES

SECTION 9: CONTACT INFORMATION

SECTION 10: OTHER INFORMATION

SECTION 11: INDEX

SECTION 12: GLOSSARY

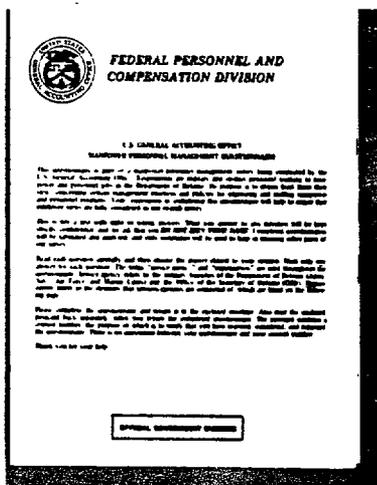
SECTION 13: REFERENCES

SECTION 14: CONTACT INFORMATION

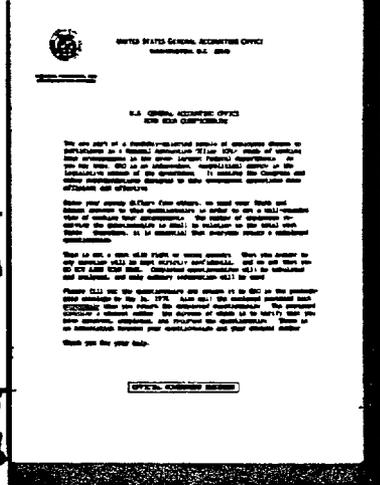
SECTION 15: OTHER INFORMATION

**INVENTORY OF FPCD MACHINERY**

# FPCD SURVEYS INVOLVING COMPUTER ANALYSIS OF QUESTIONNAIRES

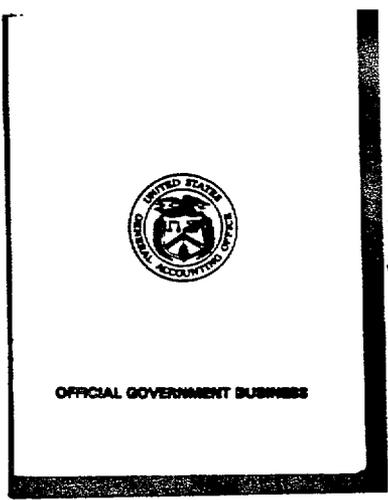
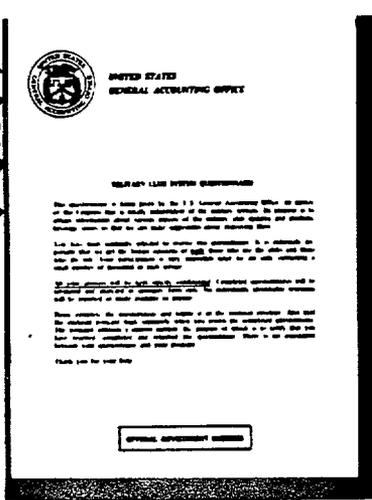


**MANPOWER/PERSONNEL MANAGEMENT IN DOD**  
**SAMPLE SIZE = 4207**  
**RETURN RATE = 87%**

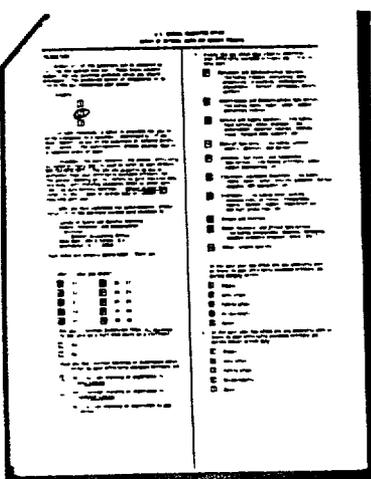


**FEDERAL HOURS OF WORK**  
**SAMPLE SIZE = 3609**  
**RETURN RATE = 87%**

**USE OF MILITARY CLUBS**  
**SAMPLE SIZE = 4708**  
**RETURN RATE = 78%**

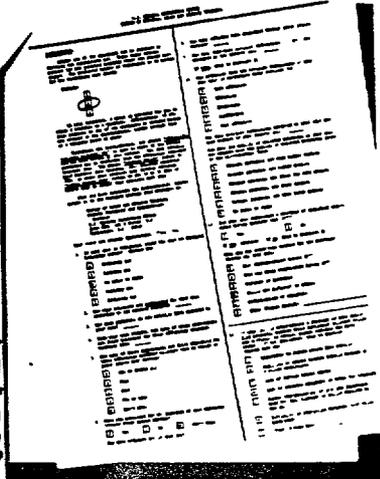


**EEO PRACTICES IN THE DEPARTMENT OF JUSTICE**  
**SAMPLE SIZE = 3574**  
**RETURN RATE = 78%**



**NATIONAL GUARD AND RESERVE TRAINING**  
**RESERVIST VERSION**  
**SAMPLE SIZE = 1835**  
**RETURN RATE = 80%**

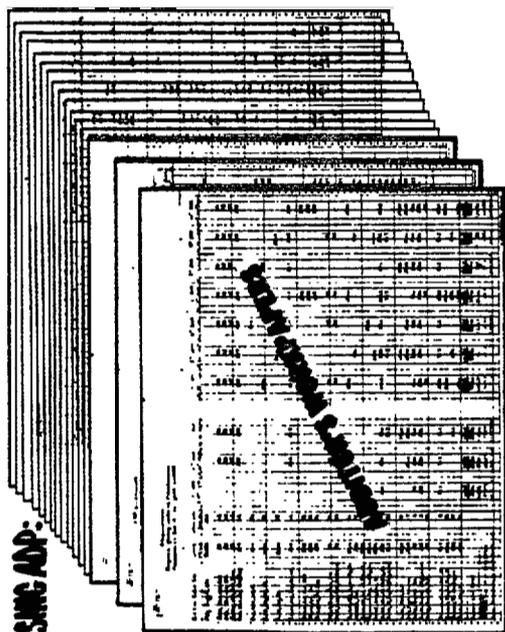
**COMMANDER VERSION**  
**SAMPLE SIZE = 1500**  
**RETURN RATE = 81%**



# ALLOCATION OF MONTHLY CLOTHING ALLOWANCES FOR MILITARY PERSONNEL

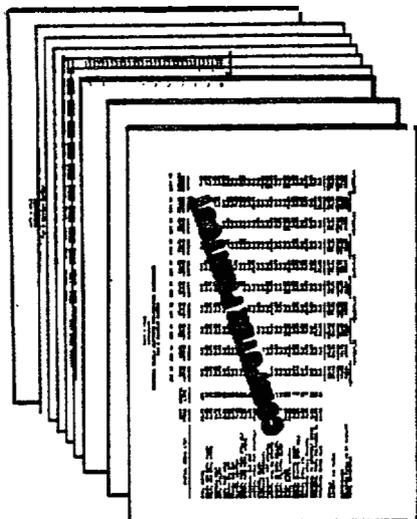
COMPARISON OF GAO SUGGESTION WITH CURRENT METHOD

WITHOUT USING ADP:



OUTPUT:

USING ADP:



COST: GS-12 SALARY (\$9176/DAY FOR 16 DAYS) \$1468

GS-12 SALARY (\$9176/DAY FOR 3 DAYS) \$275

GS-4 SALARY (\$36.08/DAY FOR 1/2 DAY) 18

ONLINE COMPUTER TIME (114 HR) 30

COMPUTER OUTPUT 100

\$423

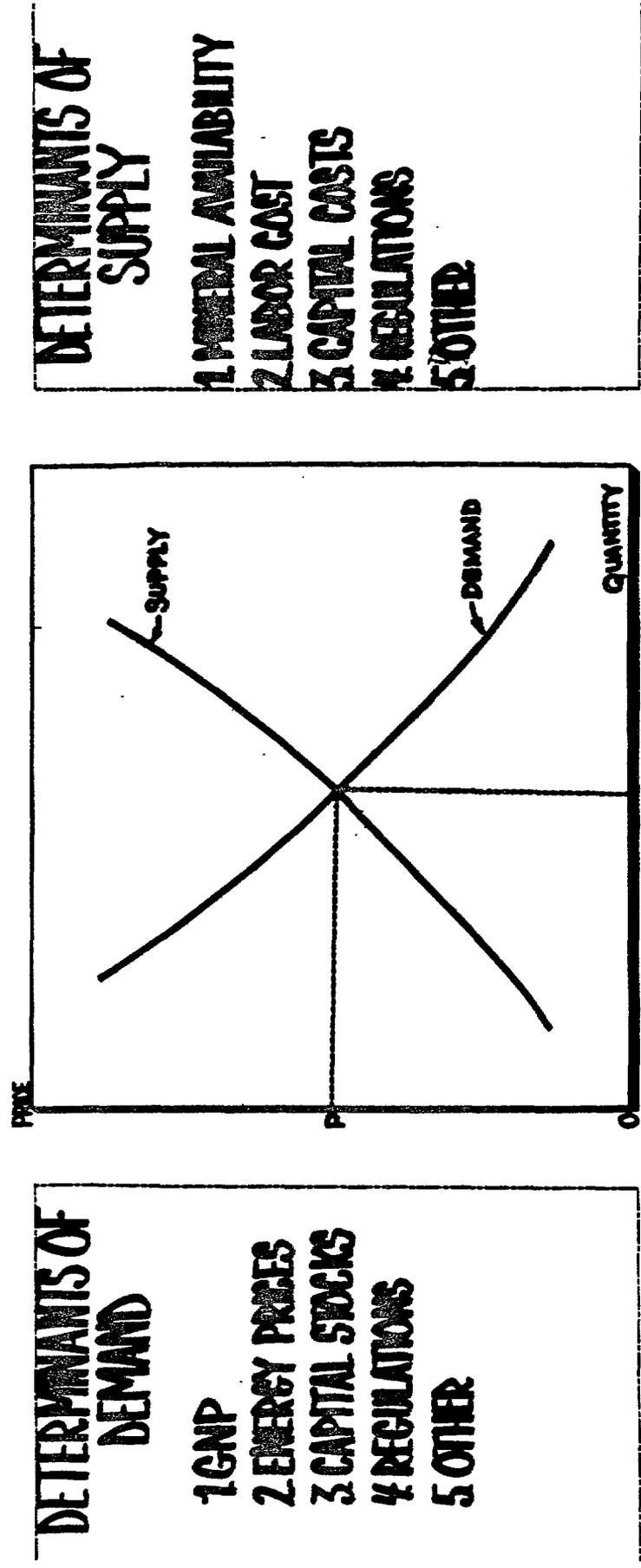
\$1468

TOTAL COST: \$1045

FPCD

\*USED GS-4 INSTEAD OF GS-12 TO ENTER DATA AND PRINTOUT PROGRAM

# EMD USES ECONOMETRIC MODELS TO ANALYZE U.S. ENERGY POLICIES



COMPLEX ECONOMETRIC MODELS REQUIRE ADP SUPPORT

### **COMPLEX ECONOMETRIC MODELS REQUIRE ADP SUPPORT**

Econometric models are basically simplified abstracts of reality. They attempt to simulate, by mathematical formulae, how things work in the real world. Such is the case with the energy models that EMD uses. We have depicted a simplified model above to show how demand and supply relationships determine the price and quantity of energy that will be produced and consumed. If any one of the demand or supply determinants are altered, the equations (represented by the supply/demand lines in the graph) will produce a different solution or equilibrium point. As a result, prices, quantities, or both may change.

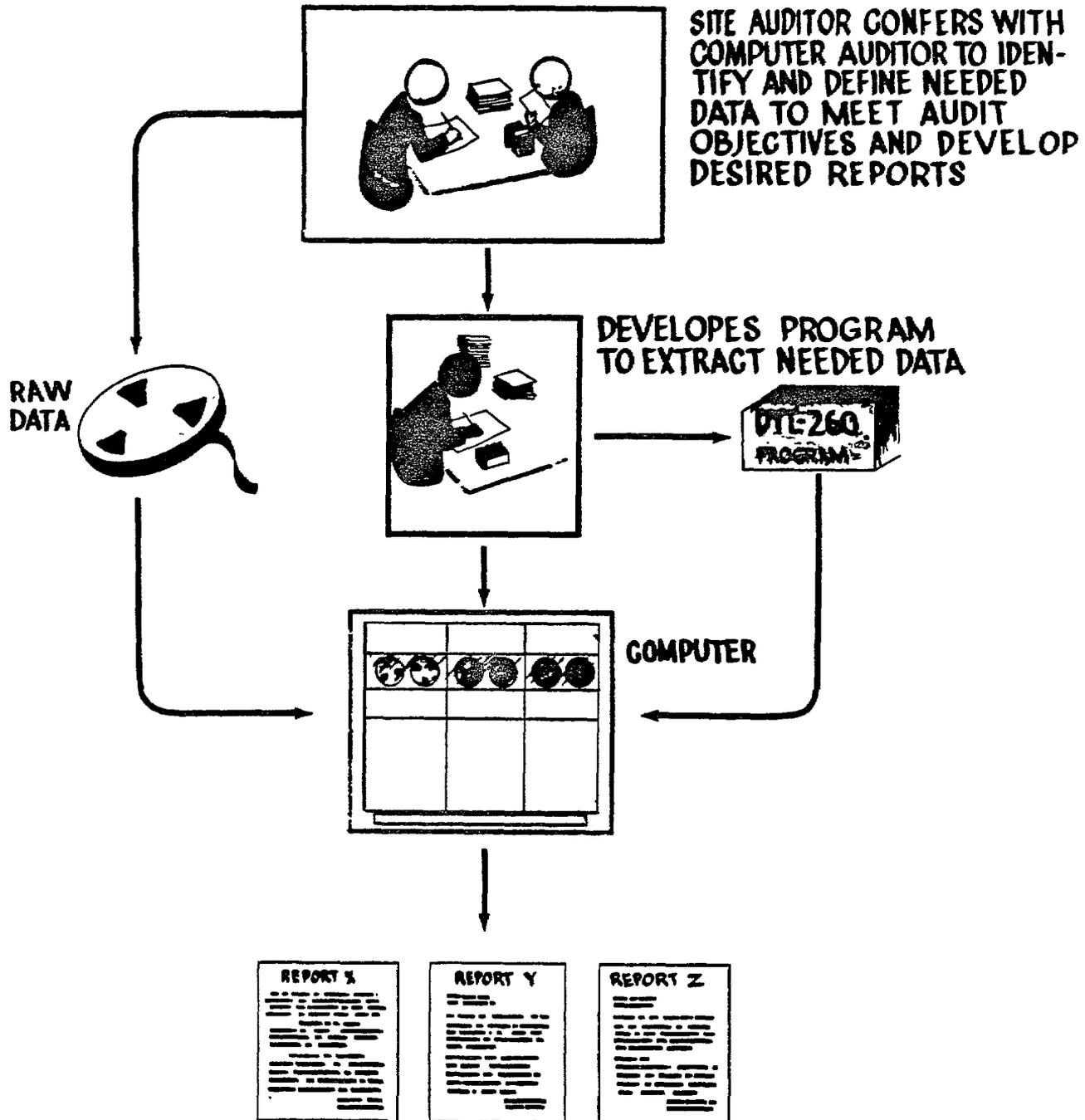
EMD uses several models in its efforts to analyze U.S. energy policy. One of these models is the Data Resources Inc (DRI) energy model. A recent forecast from the DRI energy model is attached. A quick glance at this forecast provides just a sampling of the energy variables that can be analyzed using this model. Models can not only project or forecast these variables into the future but models can also compare and contrast the effects of different energy policy scenarios.

Each model simplifies reality by incorporating assumptions. Despite this simplification process, the models' equations manipulate huge data bases which produce the energy forecast. The DRI energy model incorporates about 400 equations dealing with over 600 variables. Each variable carries with it a 20 year history or time series. It should come as no surprise then that a large computer is used to solve this model.

13.18

EMD

# GENERAL GOVERNMENT DIVISION COMPUTERIZED INFORMATION RETRIEVAL



DESIRED DATA PRODUCED

GGD

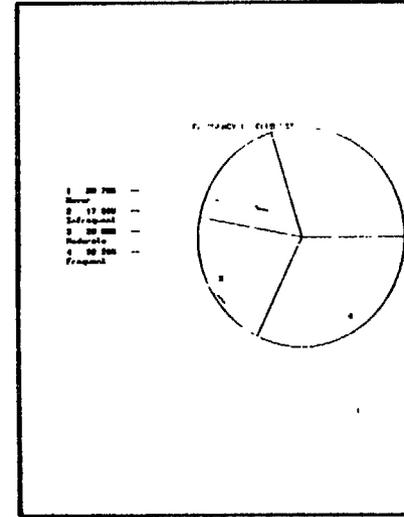
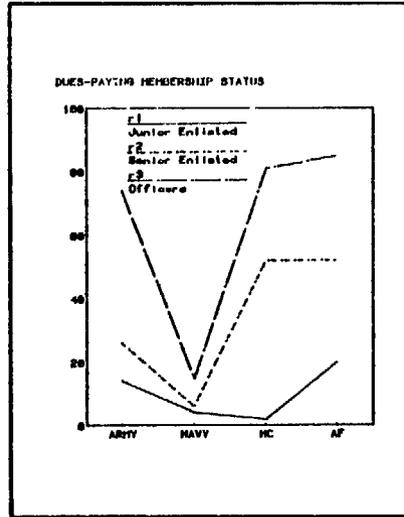
# CAMERA READY GRAPHICS

## RAW DATA

MEMBER STATUS				
MEMBER	1971	1972	1973	1974
ACTIVE	10.1	10.5	10.4	10.3
RESERVE	11.2	10.8	10.6	10.5
RETIRED	10.8	10.4	10.3	10.2
TOTAL	32.1	31.7	31.3	31.0

DUES-PAYING MEMBERSHIP STATUS				
MEMBER	1971	1972	1973	1974
ACTIVE	10.1	10.5	10.4	10.3
RESERVE	11.2	10.8	10.6	10.5
RETIRED	10.8	10.4	10.3	10.2
TOTAL	32.1	31.7	31.3	31.0

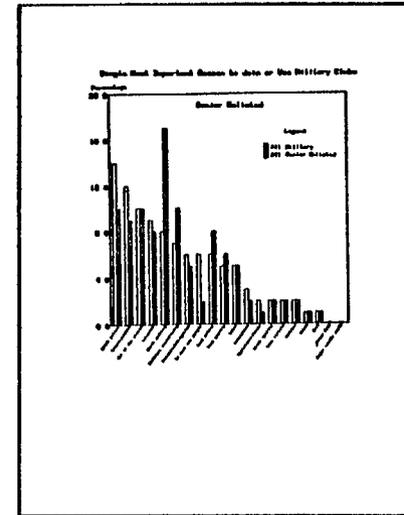
## GRAPHS PRODUCED BY COMPUTER (USING TEXTRONIC AND INFONET)



SINGLE NAVY MEMBERSHIP STATUS BY AGE CLASS					
	18-24	25-34	35-44	45-54	55-64
Check making services	11	4	2	2	11
Mail postage	10	1	1	1	1
Smoking with military personnel	10	0	0	0	0
Out of town phone	10	1	1	1	1
Available	10	1	1	1	1
Entertainment	10	1	1	1	1
Spouse (from residence)	10	1	1	1	1
Food prices	10	1	1	1	1
Food quality	10	1	1	1	1
Freedom of navigation in port	10	1	1	1	1
Other	10	1	1	1	1
Attitude/employee attitude	10	1	1	1	1
Mail service	10	1	1	1	1
Other quality	10	1	1	1	1
Alcohol/beer	10	1	1	1	1
Place to meet new people	10	1	1	1	1
Means of operation	10	1	1	1	1
Political opposition/beer	10	1	1	1	1
Attitude	10	1	1	1	1
Amount of food	10	1	1	1	1
Discipline	10	1	1	1	1
Use of better credit cards	10	1	1	1	1

## ADVANTAGES

- TIME - ABOUT 10 MINUTES/GRAPH
- COST - ABOUT \$6.00/GRAPH (INCLUDING LABOR)
- MODIFICATIONS CAN BE DONE QUICKLY WITH MINIMAL COST
- EXCELLENT FLEXIBILITY
- LEARNING TIME - HOURS
- MINIMAL ADP KNOWLEDGE REQUIRED



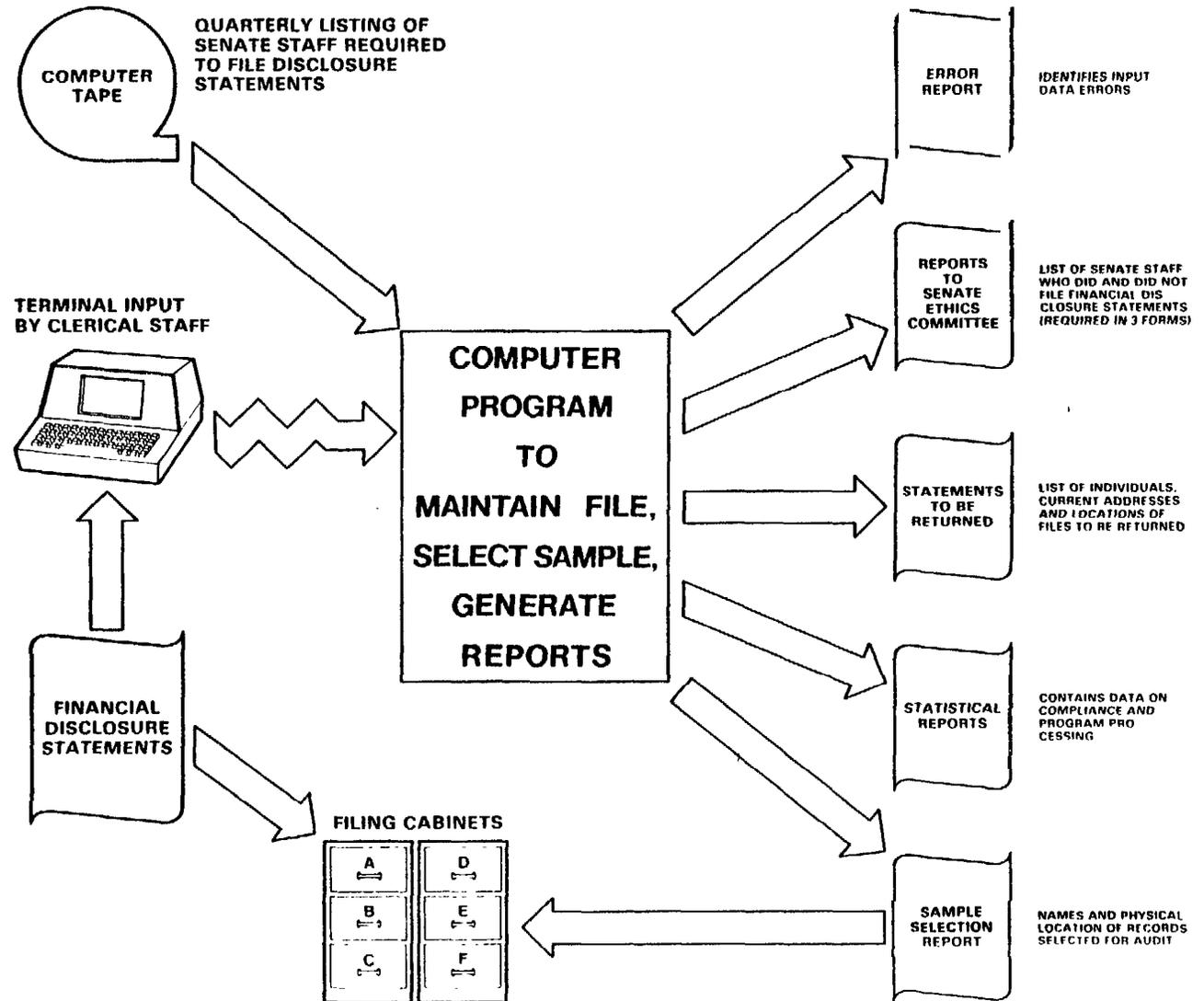
# DATA BASE MANAGEMENT SYSTEM (DBMS) FOR FINANCIAL DISCLOSURES

## SYSTEM REQUIREMENTS

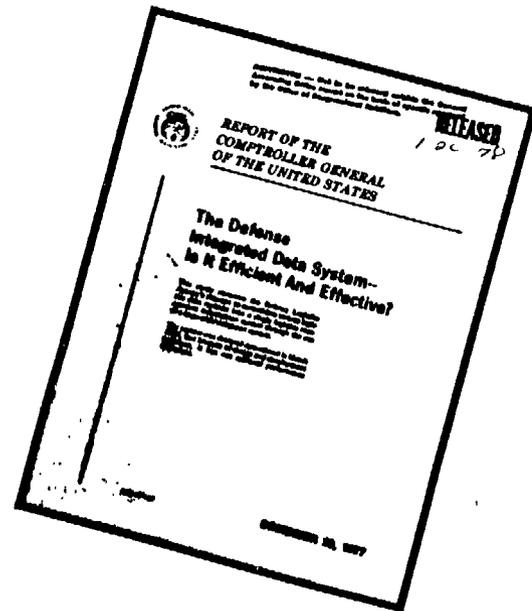
1. MAINTAIN A RECORD OF FINANCIAL DISCLOSURE STATEMENTS FOR 7 YEARS
2. SELECT A SAMPLE OF SENATE STAFF FOR AUDIT
3. PROVIDE REPORTS FOR THE SENATE ETHICS COMMITTEE
4. PROVIDE A MEANS FOR UPDATING INFORMATION
5. PROVIDE STATISTICS AS REQUIRED UNDER SENATE RESOLUTION - 110
6. IDENTIFY PHYSICAL LOCATION OF FINANCIAL DISCLOSURE STATEMENTS

13.21

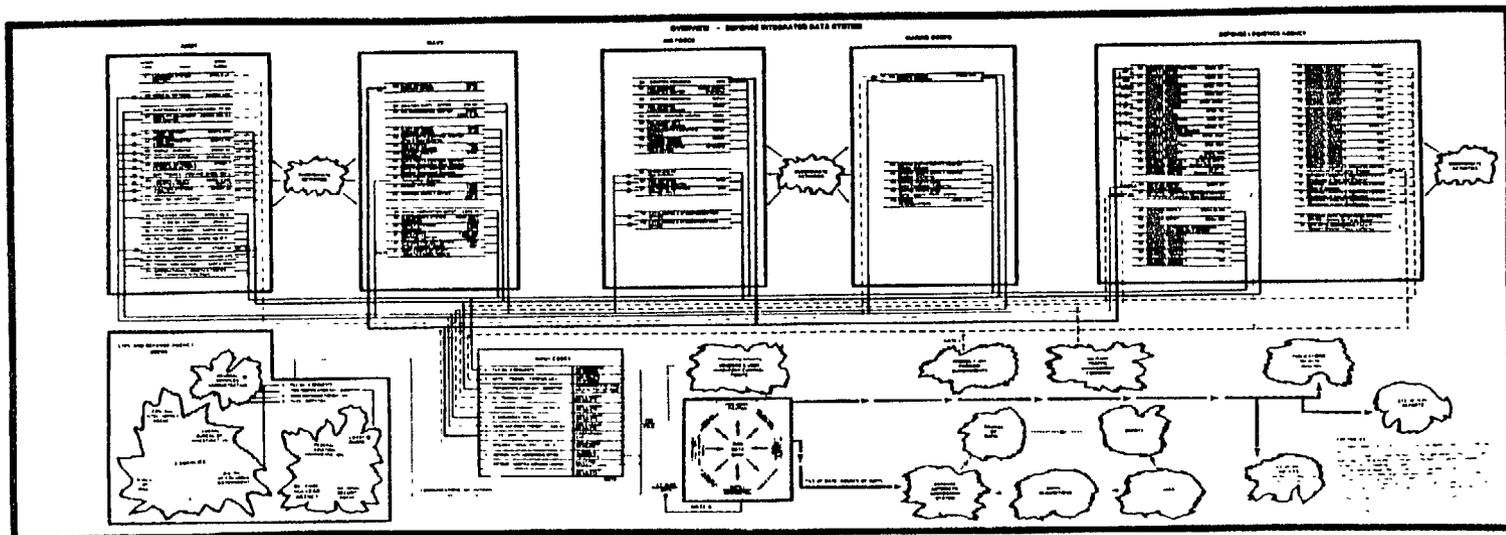
FPD



# GAO DEVELOPED DATA FLOW MODEL OF THE DEFENSE INTEGRATED DATA SYSTEM (DIDS), A MAJOR MILITARY LOGISTICS ADP SYSTEM.



13.22



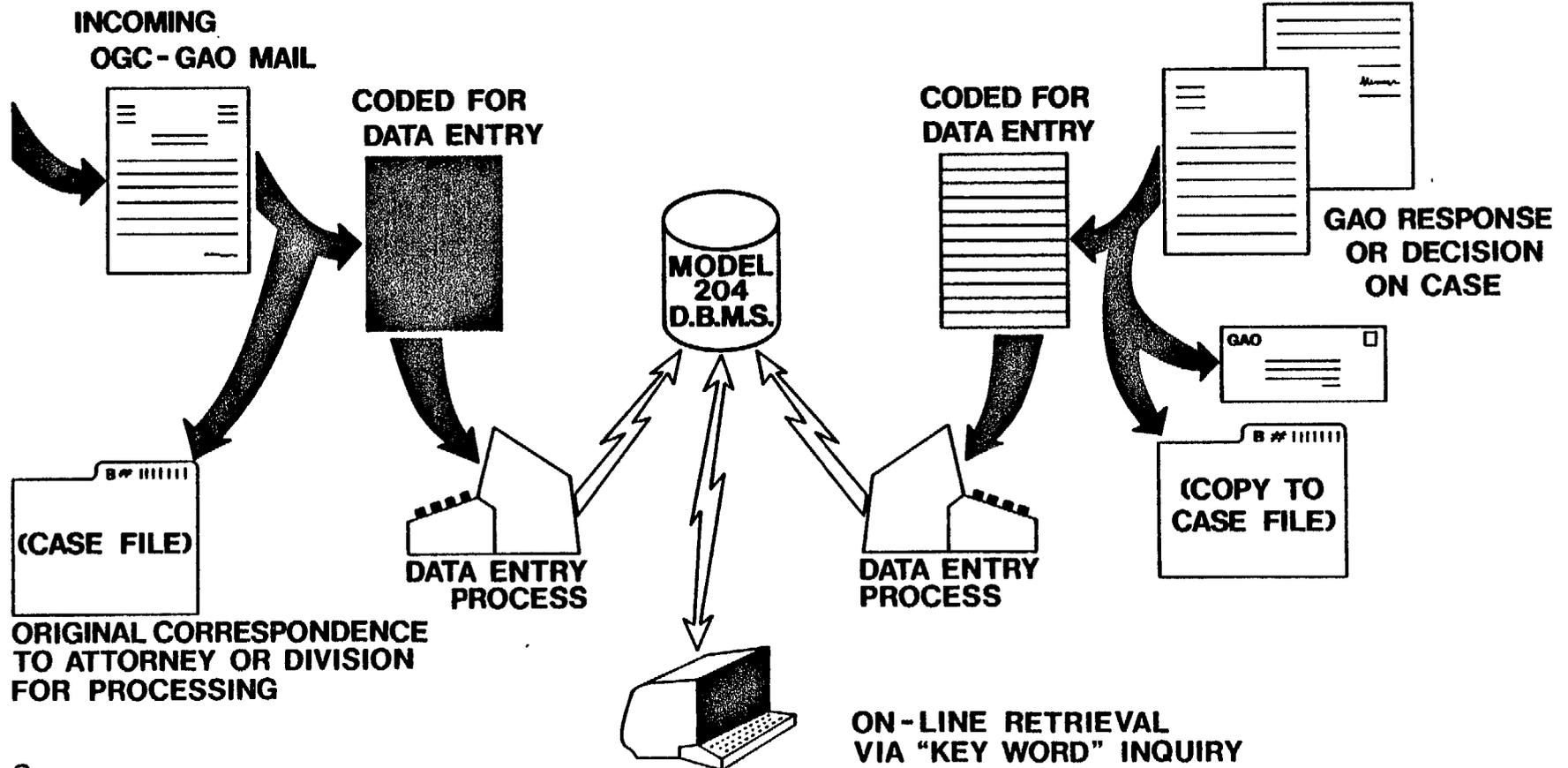
LCD

# - OGC - LIRS -

## CORRESPONDENCE CONTROL SYSTEM

### INCOMING CORRESPONDENCE

### OUTGOING CORRESPONDENCE



13.23

OGC

# EFFECTIVENESS/CREDIBILITY OF ADP/MODELING

## OUTSIDE GAO

- USING AGENCY'S MODEL WITH VARYING INPUTS INCREASES EFFECTIVENESS (E.G. A-76)
- VALIDATING A DIFFERENT MODEL BY USING AGENCY'S INPUTS TO OBTAIN AGENCY'S OUTPUT INCREASES CREDIBILITY (E.G. A-10 AIRCRAFT)
- DEVELOPING BETTER MODELS AND GIVING PAPERS AT PROFESSIONAL MEETINGS INCREASES GAO EFFECTIVENESS & CREDIBILITY (E.G. MORS DAVID RIST PRIZE)

## INSIDE GAO

- 3 REPORT LEVELS NEEDED TO ESTABLISH CREDIBILITY

<u>LEVEL</u>	<u>CONTENTS</u>	<u>CUSTOMER</u>
I	DETAILS OF MODEL; INPUTS	GAO PROFESSIONAL; AGENCY; ADP OR/SA COMMUNITY
II	DESCRIPTION OF MODEL RESULTS; ANALYSIS	TEAM DIRECTOR; TEAM LEADER
III	BRIEF SUMMARY (FEW OR NO NUMBERS)	LAY READER; ULTIMATE CUSTOMER

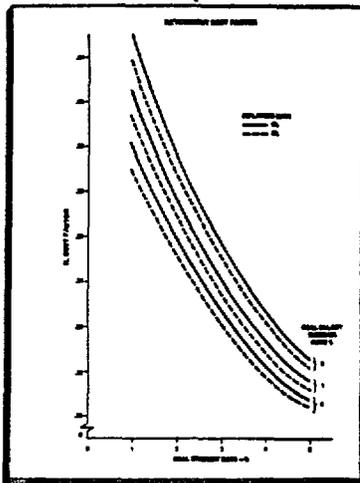
# AUDITS USING THE COMPUTER

## (MANAGEMENT EFFICIENCY AND EFFECTIVENESS)

A-76

### CONTRACT OUT?

EVALUATED & AUTOMATED CSC PROCEDURE CONSISTING OF SEVERAL PROGRAMS + HAND CALCULATIONS. WROTE ONE PROGRAM HANDLING SETS OF INFLATION RATES, INTEREST RATES, & SALARY INCREASE RATES.



NOW USED BY GAO TO EVALUATE SPECIFIC INSTALLATIONS

### DATA BASE

#### SEARCHING OR LISTING

- DOD350 CONTRACT AWARDS
- PROCUREMENT DATA
- CIVIL PROCUREMENT ON TAPE, UPDATED YEARLY

↓

Contract No.	Title	Amount	Start Date	End Date	Status
...	...	...	...	...	...
...	...	...	...	...	...
...	...	...	...	...	...

Contract No.	Title	Amount	Start Date	End Date	Status
...	...	...	...	...	...
...	...	...	...	...	...
...	...	...	...	...	...

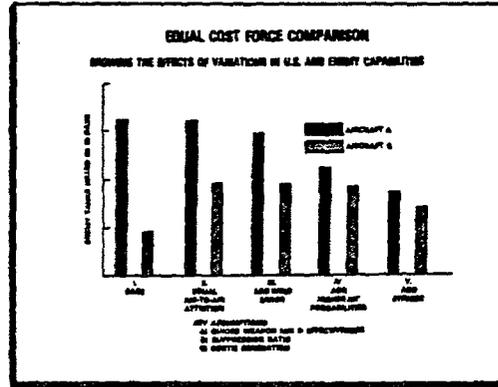
Contract No.	Title	Amount	Start Date	End Date	Status
...	...	...	...	...	...
...	...	...	...	...	...
...	...	...	...	...	...

PSAD

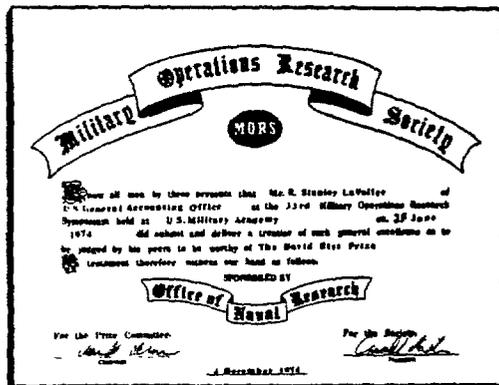
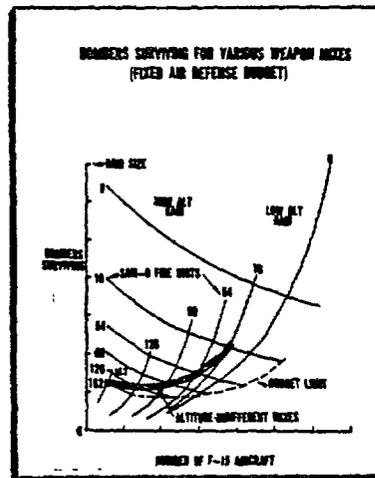
# AUDITS USING COMPUTER MODELS

## (PROGRAM RESULTS)

ATTACK HELICOPTER  
 A-10 AIRCRAFT →  
 PATRIOT AIR DEFENSE SYSTEM  
 AIR DEFENSE MISSION



**MODEL CAPABILITIES**  
 OPTIMIZES ATTACKERS STRATEGY  
 FINDS BEST DEFENSE MIX FOR GIVEN BUDGET  
 CAN FIND BEST INFERENCE MIX (IN VS. LO ALT. ATTACK)  
 CHEAP & FAST TO RUN  
 COST MODEL FLEXIBLE  
 DEFENSE MIX CAN INCLUDE AIRCRAFT AS WELL AS GROUND WEAPONS



PAPER WON PRIZE

PSAD



A live demonstration conducted by Nancy Simmons of the FPC Division. It showed how a computer-connected terminal is used in the analysis of data and the documentation of results required by a typical audit assignment.