Chapter 1
Summary

Contents

Page

Introduction 3

Management of Information Technology 3
Strategic Planning 4
Information Availability and Data Quality 4
Innovation 4
Procurement 5
Information Resources Management (IRE) 5

Information Systems Security and Computer Crime.... 6
Information Systems Security 6
Computer Crime 6

Information Technology and Decision Support. 7

Management of Government Information Dissemination 9

Information Technology and Congressional Oversight 10

In Conclusion 10

Chapter 1

Summary

INTRODUCTION

Information technology-including computers, software, telecommunications, and the like-is critically important to the functioning of the U.S. Government. By any measure, the Federal Government-with its roughly 27,000 mainframe computers, over 100,000 microcomputers, and over 170,000 mainframe computer terminals[1]–has the largest inventory of computer equipment of any single organization or government in the world.

However, much of the policy framework previously established by Congress to control, oversee, and encourage the management and use of Federal information technology has been overtaken by the rapid pace at which new technology applications, issues, and opportunities are being generated.

In addition, the Federal Government is not maximizing the return on its substantial information technology investment (conservatively estimated at $60 billion over fiscal years 1982-86[2]) with respect to improving: 1) the efficiency of government in delivering services; 2) the security and privacy of information maintained in computerized systems; and 3) the quality of government management itself. Also, the congressional intent as originally embodied in laws such as the Paperwork Reduction Act, Freedom of Information Act, Privacy Act, Public Printing Act, and Omnibus Crime Control Act is not being fully carried out due in part to new technological applications and issues not envisioned at the time of enactment.

[1]Unless otherwise noted, statistics cited in this chapter are based on the OTA Federal Agency Data Request that was sent to the 13 cabinet departments and 20 selected independent agencies, and to which 142 agency components responded. See app. B for a list.

[2]Based on Office of Management and Budget (OMB) data. Does not include some telecommunication costs or information technology activities that are classified or embedded in other agency programs.

MANAGEMENT OF INFORMATION TECHNOLOGY

The management of Federal Government information technology has received high-level congressional and executive branch attention for at least two decades, with a new round of studies, reports, and policy initiatives every several years. Management issues involving planning, procurement, security, and the like must be revisited periodically because of the dynamic nature of the technology and changing applications.

Major studies from the Coremission on Federal Paperwork in 1977 through the Grace Commission in 1983 reported on needed improvements in Federal information technology management. In the last few years, the Office of Management and Budget (OMB), General Services Administration (GSA), and various individual agencies have taken numerous management initiatives. And most recently, OMB has given attention to information technology management both as part of overall government management and through specific actions such as the December 1985 circular on "Management of Federal Information Resources."3

Nonetheless, OTA identified several further needs for management improvement that appear to be crucial to realizing the full poten-

[3]See Office of Management and Budget, *Management of the United States Government Fisca) Year* 1986, and OMB, Circular A-1 30 on "Management of Federal Information Resources," issued Dec. 12, 1985. Also see OMB, *Management of the United States Government Fiscal Year 1987.*

tial of information technology for increasing the efficiency and effectiveness of government. These are discussed briefly below. Many of these needs could be met by the executive branch acting alone. However, Congress can facilitate, encourage, and, where necessary, require these actions.

Strategic Planning

The annual "5-year plans" currently published by OMB (as mandated by the Paperwork Reduction Act) have several significant deficiencies. While the documents are gradually becoming more comprehensive, they are not "plans," and they do not analyze strategies for using information technology to further government missions, either on a governmentwide or individual agency basis. There is no real vision of the future and little discussion of alternative strategies for use and management of information technology.

Despite some more recent efforts to develop thoughtful plans, many agency planning efforts still have some major flaws, including a failure to:

- include strategic as well as operational plans;
- identify innovative opportunities for use of information technology;
- connect planning effectively to implementation;
- involve users, clients, and the interested public in the planning process; and
- explicitly consider the implications of information technology use for protection of information security and privacy.

One vehicle available to Congress for implementing improvements in planning (and other areas) is the Paperwork Reduction Act of 1980, which in part established an information technology management framework for the government. The act is overdue for reauthorization and could be amended to provide a more precise mandate on the strategic planning process and the contents of the 5-year plans.

Information Availability and Data Quality

The weaknesses of the 5-year plans are compounded by serious deficiencies in the scope and quality of information available to Congress, and to the agencies themselves, on key Federal information technology trends and applications. These deficiencies can hamper effective congressional oversight and agency decisionmaking. For this study, in the absence of much needed information, OTA conducted its own survey of Federal agency use of information technology (see app. B for discussion of OTA's Federal Agency Data Request).

A related problem is that the results of General Accounting Office (GAO) audits, computer matches of various Federal record systems, and a variety of other internal and external audits and studies indicate that the quality (completeness and accuracy) of data and records in Federal computerized systems varies widely—from quite good to very poor.[4] Agency (and congressional) decisions based on inaccurate and incomplete information can lead to wasteful or even harmful results or to missed opportunities and failure to identify key problems.

OTA found that there is a need: 1) to specify the types of information that should be reported on a periodic or continuous basis in order to assist both congressional and central agency oversight of Federal information technology, and 2) to strengthen the data quality standards and procedures applicable to computerized Federal systems.

Innovation

Where OTA identified examples of agency innovation-such as the use of electronic mail, videoconferencing, and computer-based decision support—the exchange of this experience

[4]For further discussion of Federal record quality, see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy, 1986* forthcoming.

and learning with other agencies appeared to be irregular or nonexistent. A common institutional problem is that many agencies either believe that publicizing innovation is "just asking for trouble' or view many innovations as too risky to try at all.

OTA concluded that actions to encourage agency innovation are needed, such as: establishing informal and formal mechanisms to exchange experiences gained and lessons learned; developing guidelines that provide agencies with room to innovate, but also help detect and resolve emerging issues before they impair the innovation process; and possibly designating a Federal information technology innovation center (or centers).

Procurement

Government information technology procurement is subject to multiple and sometimes conflicting efforts to simultaneously expedite the procurement process (e.g., through GSA's delegation of procurement authority), increase the level of competition (e.g., through congressional enactment of the Competition in Contracting Act), and more clearly demonstrate a significant return on investment in information technology (as now required by OMB).

OTA concluded that it is too early to fully assess the overall impact of these procurement initiatives. However, there is considerable evidence of reduced technological obsolescence over the last 10 years. For example, Federal agencies responding to the OTA survey reported, collectively, a reduction in percentage of Federal mainframe computers over 6 years old from about 60 percent in 1975 to 10 percent in 1984; and an increase in mainframe computers under 3 years old from 30 percent in 1975 to 60 percent in 1984.

Beyond the availability of relatively new equipment, the "success" of procurement is closely tied to the government's ability to plan and define technology needs and to match technology to those needs. It is in this area particularly that problems persist, especially with the larger systems, such as at the Internal Revenue Service and Social Security Administration.[5] There still appears to be a need for: better training of procurement staff, greater senior management involvement in and understanding of the planning and procurement process, improved mechanisms to exchange procurement experience and learning, and possibly a procurement and management troubleshooting team to assist with serious trouble spots.

Information Resources Management (IRM)

In enacting the Paperwork Reduction Act (PRA), Congress directed that each agency designate a high-level official responsible for all aspects of the management of information technology. The information resources management (IRM) concept was intended to bring together previously disparate functions-such as computers, telecommunications, office auto mation, and the like-and to establish the importance of information as a resource.

OTA found that, while agencies have designated an IRM officer, actual implementation of IRM varies widely and has been only partially or minimally implemented in many agencies. And the Paperwork Reduction Act provides limited or no direct guidance in some key areas such as: the use of information technology to support agency decisionmaking (e.g., computer-based decision support), and public information technology and policy (e.g., electronic databases and electronic dissemination of government information). OTA concluded that there is a need to review progress in PRA implementation since 1980 and clarify the scope of authority and responsibilities intended for IRM officers.

[5] 0TA is conducting a separate in-depth case study entitled *Federal Government Information Technology: Case Study of the Social Security Administration,* forthcoming in summer/fall 1986.

INFORMATION SYSTEMS SECURITY AND COMPUTER CRIME

Information Systems Security"

An important management responsibility is maintaining the security of information systems. If proper security is not maintained, the government cannot assure: 1) the continuity and effectiveness of government operations; 2) the quality (e.g., accuracy and completeness) of information in Federal systems; or 3) control over those types of information (e.g., personal, proprietary, classified) to which access is limited by law or regulation.

The proliferation of microcomputers, continuing rapid increase in mainframe computer systems, large percentage of computerized Federal records (e.g., about 80 percent of Privacy Act records are maintained in fully or partially computerized systems), and growing use of electronic data linkages of all sorts, clearly have increased the difficulty and complexity of protecting government information. Information systems security is now recognized as a serious problem by both civilian and military agencies; the President emphasized information systems security in the September 1984 National Security Decision Directive (NSDD) 145, as has OMB in its December 1985 information management circular.

There is, indeed, cause for concern. OTA found that agencies are often not implementing the measures mandated or suggested under prior policy guidance. For systems that process sensitive but unclassified information, OTA found that:

- about 40 percent of agencies responding have not conducted a risk analysis during the last 5 years, 25 percent do not screen personnel with computer access, and 50 percent do not screen computer applications for sensitivity;
- in addition, about 40 percent of agencies do not use audit software or restrictions on dial-up (remote) access to mainframe computers, and about 80 percent do not use encryption; and
- finally, about 75 percent of agencies responding do not have an explicit security policy for microcomputers, and about 60 percent do not have (and are not developing) contingency plans for use if mainframe computers are disrupted.

The Administration's approach, through NSDD 145, has been to assign a much stronger role to the military and to the National Security Agency (NSA) in particular. While this may well strengthen Federal leadership in information systems security, it also puts the national security community in an unusual, influential if not controlling position on this key aspect of information policy, and could heighten tension between the defense and civilian sectors.

OTA identified several options on information systems security that warrant consideration, including:

- designating a civilian agency to provide information security training and technical support to the civilian sector (similar to NSA's role in the defense sector);
- changing budget procedures to provide more visibility for computer and telecommunications security in agency budget requests (i.e., a security line item); and
- codifying part or all of NSDD 145 into law, clarifying the roles of NSA and civilian agencies so as to remove the possibility that national security agencies might have undue control over civilian agency functions.

Some of these options are reflected, at least in part, in H.R. 2788, the "Computer Security Research and Training Act of 1985, " as amended.

Computer Crime

One purpose of good security is, of course, to protect against criminal activity directed towards computer systems and the information they contain. Technical and administra-

'For further discussion of technical security options, see the OTA study on New *Communications Technology: Implications for Privacy and Security* is expected to be completed in winter 1986-87.

tive measures are important parts of good security. But, in addition, criminal laws on computer abuse can provide another disincentive for potential violators and facilitate prose cution when crimes occur.

Since the 1970s, there has been a growing consensus that existing criminal laws covering the variety of crimes that can be committed with a computer (e.g., fraud, theft, embezzlement, invasion of privacy, trespass) either do not cover some computer abuses, or are not strong and clear enough to discourage computer crimes and allow expeditious prosecution. The available evidence suggests that significant losses have occurred. However, the total volume and severity of computer crime is unknown, given a scarcity of reliable information. Nonetheless, the potential (if not current) problem is thought to be so serious that 45 States and, in 1984, the Federal Government, have enacted computer crime laws.

Congress could fine-tune this Federal law (Computer Fraud and Abuse Act of 1984), giving particular attention to the following areas, among others: extending the coverage to private sector computers operating in interstate commerce (currently only Federal computers and those operated by certain financial institutions are covered); refining any overly broad language (e.g., with respect to unintentionally restricting computerized dissemination of or access to public information); and establishing a mandatory computer crime reporting system for Federal agencies (OTA found that only about one-fifth of agencies have a computer crime tracking system or procedures).

OTA found that because many Federal (as well as private) computer systems have computers located in more than one State and/or use data communication networks that routinely cross State lines. State jurisdiction can be hard to establish, given the dynamic nature of computer/communications linkages. On this basis, OTA concluded that some form of interstate Federal computer crime law is warranted.

In general, OTA concluded that effective computer crime legislation needs to balance concerns about the potentially serious nature of such crime with other factors, such as:

- the responsibilities of vendors, owners, and users for the security of their systems;
- the need for effective administrative and technical security measures;
- the need to balance Federal and State roles in the prosecution of computer crime;
- consistency with other aspects of Federal information policy (e.g., Privacy Act, Freedom of Information Act, Omnibus Crime Control Act); and
- consistency with State computer crime laws.

Several of these and other factors are reflected in legislation under active congressional consideration, including: H.R. 1001, “Counterfeit Access Device and Computer Fraud and Abuse Act of 1985”; H.R. 930, “National Computer Systems Protection Act of 1985”; S. 440, “Computer Systems Protection Act of 1985”; S. 610, amendment to Computer Fraud and Abuse Act; and S. 1678 (and H.R. 3381), “Federal Computer Systems Protection Act of 1985. ”

INFORMATION TECHNOLOGY AND DECISION SUPPORT

One of the less visible but important applications of information technology is to support decisionmaking. In the context of the Federal Government, this could include decisions about governmentwide or agency-specific policies, plans, priorities, budgets, and/or program implementation options. The range of possible applications includes, for example: the use of simple spreadsheet software on microcomputers to help analyze budget options; the running of complex simulation models to better understand the possible impacts

of alternative program strategies; the collection and synthesis of information from several electronic databases relevant to the decision at hand; the use of computer graphics to analyze and display key trend and foresight information; and participation in decision conferences where decisionmakers (and staff) use computer and analytical tools to help work through a decision problem.

At the outset of this study, OTA found little systematic information on the use of computer-based decision support in the Federal Government. Computer modeling and electronic databases are not included within the purview of senior IRM officials as their responsibilities are commonly defined. Nor does the language or legislative history of the Paperwork Reduction Act provide guidance as to whether these information technology applications were intended to be included within IRM.

The results of OTA's Federal Agency Data Request provide a profile of the extent and use of these techniques. For example:

- about 60 percent of Federal agency units report at least some use of computer modeling, frequently for decision support (but also for research and scientific purposes), with the number of applications ranging up to 2,000 per agency component; and
- use of computer-based decision analytic techniques appears to have increased dramatically since the advent of microcomputers:
  - —about 90 percent of Federal agency units report use of spreadsheet software;
  - —about half use quantitative decision techniques (e.g., linear programming, systems analysis, critical path analysis);
  - —about one-fourth use forecasting techniques (e.g., regression analysis) and quantitative decision analytic techniques; and
  - —about one-twentieth use computer-assisted decision conferences and/or computer conferencing.

Overall, executive branch officials believe these techniques to be very useful, even essential, to agency decisionmaking. However, few can document this claim other than by citing ad hoc examples, because there has been little research on the impact of decision support techniques on agency decisionmaking and little effort to exchange experience among agencies using these techniques.

OTA identified several possible actions that could help to: 1) improve sharing of expertise and learning about computer-based decison support; 2) facilitate congressional and public access where appropriate; 3) enhance understanding of the strengths and limitations, uses and abuses of computer modeling and electronic databases; and 4) improve the government's return on a significant investment. Possible actions that warrant consideration include:

- establishing guidelines or standards for model documentation, verification, and validation (at least for major models);
- establishing directories or indices to major computer models and electronic databases;
- clarifying procedures on congressional and public access to agency computer models and databases;
- conducting further research on the impact of computer-based decision support on agency decisionmaking;
- conducting further testing and development of the decision conference technique;
- developing a formalized foresight capability in major agencies; and
- establishing clear institutional responsibility for some or all of the above, possibly by including decision support as part of information resources management.

A significant, unrealized potential of information technology is to improve the foresight capability of the government. Foresight can be viewed as a component of decision support that involves monitoring and analyzing key longer term trends and their implications for government policies and programs. The combination of computer modeling, electronic data collection, and various decision analytic tech-

niques used in a decision conference format may be an effective technical approach to improve governmentwide foresight capability, when coupled with institutional mechanisms that cut across agency and disciplinary lines. OTA identified several possible actions to help accomplish the latter, ranging from: bringing foresight into the scope of information resources management, to including foresight functions as part of agency decision support centers, to establishing separate foresight offices organized by agency or by subject matter, and to setting up a governmentwide foresight office that would pull together key trends information from the various agencies (as envisioned in S. 1031, the Critical Trends Assessment Act of 1985).

MANAGEMENT OF GOVERNMENT INFORMATION DISSEMINATION

Information technology holds out the promise of faster, cheaper, and more efficient collection (e.g., through computer-aided surveys and document filings), maintenance (e.g., in computerized databases and optical disks), and dissemination of government information (e.g, via electronic mail, interactive data networks, electronic bulletin boards, remote printing-on-demand, and computer tape exchange). OTA's preliminary research in this area suggests that the Federal Government is at or near the threshold of a major shift toward greater use of information technology for managing government information. These technologies could revolutionize the public information functions of the government.

At the same time, because government information is vital to so many users—in and outside of government-and central to numerous public laws and agency missions, the impending shift is raising a wide range of policy issues. The issues are complicated because of perceived tensions between:

- public access and the public's right to know (as embodied in the Freedom of Information Act) and the role of Federal agencies in actively disseminating public information (as mandated in the Public Printing Act and numerous authorizing statutes);
- management efficiency and cost reduction (per OMB circulars, the Deficit Reduction Act, and, to some extent, the Paperwork Reduction Act); and
- particularly for scientific and technical information, national security and foreign trade concerns.

OTA concluded that further research in this area is warranted, but that, ultimately, Congress is likely to be called on to update existing public information laws and address a variety of trends and issues such as:

- reduction of paperwork and publications;
- increasing use of electronic dissemination;
- cost-effectiveness of electronic information options;
- equity of access to government electronic information;
- private sector role in Federal electronic information activities;
- institutional responsibility for government information collection, dissemination, policy, and operations;
- need for a public information index or clearinghouse;
- mechanisms for exchange of learning and innovation;
- Freedom of Information Act implementation;
- electronic recordkeeping and archiving;
- scientific and technical information exchange; and
- other issues such as transborder information flow, depository library system, Federal statistical system, and copyright protection.

INFORMATION TECHNOLOGY AND CONGRESSIONAL OVERSIGHT

This report focuses primarily on executive agency management and use of information technology, and congressional oversight thereof. The trends, issues, and options discussed are properly within the purview of congressional oversight of executive branch programs, activities, and implementation of public laws. However, information technology also has a potential role in the actual conduct of congressional oversight.

Congress as a whole has made great strides over the last 10 to 15 years in using information technology with respect to legislative information retrieval, constituent mail and correspondence management, and some administrative functions. However, the use of information technology for direct support of policymaking and oversight is just beginning.

OTA identified significant unrealized opportunities for congressional use of information technology in conducting oversight, and an apparent lack of clear strategy for such use. A similar situation exists at the State level, based on an OTA review of relevant activities in nine State legislatures (California, New York, Wisconsin, Minnesota, Florida, Washington, Texas, Virginia, and South Dakota).

Four specific opportunities identified by OTA include: 1) direct access by congressional committees and staff to agency electronic files; 2) use of computer-based modeling and decision support; 3) video- and computer-conferencing to augment committee and staff oversight activities; and 4) electronic tracking of agency and executive actions. Congress may wish to plan and conduct a series of pilot tests and demonstrations in each of these areas, in order to more accurately assess the benefits, costs, and problems.

The pilot test approach has worked in the past for new technological applications in Congress. Pilot tests of congressional oversight applications should be useful to help familiarize Members and staff with new applications, identity needs for training, and develop the best match or fit between a particular application and the needs of specific committees, Members, and staff. Also, while Congress has strong constitutional powers to oversee and obtain information from the executive branch, pilot tests would help familiarize the agencies with new applications, identify any needed adjustments, and generally seek approaches that minimize possible concerns about separation of powers and executive privilege.

IN CONCLUSION

OTA's assessment of Federal Government information technology has identified significant progress, problems, and opportunities for improvement in the management and use of this very important technology. Many of the needed improvements can and ultimately would have to be implemented by the executive branch itself. Congress can facilitate and encourage appropriate actions through effective oversight and, where necessary, legislative remedies.

Chapters 2 through 8 of this report provide technical and policy analyses relevant to proposed legislation and policy initiatives on information technology management, including legislation on information systems security and computer crime noted earlier, possible amendments to the Paperwork Reduction Act and Public Printing Act, and governmentwide management initiatives such as the "Government Management Report Act of 1986. "

Appendix A to this report briefly discusses other related issues that warrant congressional attention, but are outside the primary focus of this document. Appendix B describes the methodology of and respondents to OTA's Federal Agency Data Request. Appendix C lists the OTA contractor papers relevant to this report. Appendix D lists outside reviewers and contributors.