Even though the effective use of information resources is critical to government operations, reports of studies by the Information Management and Technology (IMTEC) Division of the General Accounting Office have shown that agencies have frequently had problems in managing these resources. At the request of the Committee on Government Operations of the House of Representatives, all reports of such studies issued between October 1, 1988, and May 31, 1991, were examined. Of the 192 reports, 132 identified one or more problems relating to IRM. These reports covered information management in both the civil and defense sectors and looked at specific information systems as well as broad, government-wide issues. Massive cost overruns, inaccurate data, and poor system performance were frequently experienced. The management and operational problems described in these studies tend to fall into one of 10 different categories, with the most common problem being inadequate management of the information system development life cycle. Other problem areas include an inability to ensure the security and integrity of information systems; an inability of information systems to work together; and data that are inaccurate, unreliable, or incomplete. The first of 12 appendixes that make up the major part of this report summarizes the problem categories by type of problem and number of IMTEC reports per fiscal year, and the next 10 appendixes provide a description and examples of each category, as well as a list of reports that fell under that category. The final appendix lists the major contributors to the report.
INFORMATION RESOURCES

Summary of Federal Agencies' Information Resources Management Problems
Dear Mr. Chairman:

The magnitude and complexity of the federal government's information technology resources—the hardware, software, data, and people necessary to support the mission of an organization—require effective and efficient management. These resources are critical to ensuring the effective delivery or conduct of every major government activity. The nation's defense, revenue collection, health programs, and benefits programs all rely on information technology for developing and operating the complex systems required by these programs. Simply put, good management enhances these programs; poor management makes effective program operation impossible to achieve.

Even though the effective use of information resources is critical to government operations, our reports have shown time and again that agencies have had problems in managing these resources. At your request, we have summarized the information resources management (IRM) problems documented in previously issued reports.

To conduct our review, we examined all reports issued between October 1, 1988, and May 31, 1991, by our Information Management and Technology Division (IMTEC). Of the 192 reports that IMTEC issued during this time, 132 identified one or more problems relating to IRM. These reports covered information management in both the civil and defense sectors and looked at specific information systems as well as broad, governmentwide issues. Massive cost overruns, inaccurate data, and poor system performance were frequently experienced.

The management and operational problems described in our past work tend to fall into one of ten different categories with the most common problem being inadequate management of the information system development life cycle. Other problem areas include an inability to ensure the security and integrity of information systems; an inability of information systems to work together; and data that are inaccurate, unreliable, or incomplete. Appendix I summarizes the problem categories by type and frequency, and appendixes II through XI provide a description and
examples of each category, as well as a list of reports that fell under each category.

Our work was performed in accordance with generally accepted government auditing standards. As arranged with your office, unless you publicly announce this report's contents earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time, we will send copies to interested parties, and make copies available to others upon request.

Please contact me at (202) 336-6406 if you have any questions concerning this report. Major contributors are listed in appendix XII.

Sincerely yours,

Jack L. Brock, Jr.
Director, Government Information and Financial Management
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Letter</strong></td>
<td>1</td>
</tr>
<tr>
<td>Appendix I</td>
<td>8</td>
</tr>
<tr>
<td>Number of Reports</td>
<td></td>
</tr>
<tr>
<td>Citing Information</td>
<td></td>
</tr>
<tr>
<td>Resources Management Problems</td>
<td></td>
</tr>
<tr>
<td>Appendix II</td>
<td>9</td>
</tr>
<tr>
<td>Inadequate Management of Information Systems Development Life Cycle</td>
<td></td>
</tr>
<tr>
<td>Appendix III</td>
<td>15</td>
</tr>
<tr>
<td>Ineffective Oversight and Control of Information Resources Management</td>
<td></td>
</tr>
<tr>
<td>Appendix IV</td>
<td>19</td>
</tr>
<tr>
<td>Inability to Ensure Security, Integrity, or Reliability of Information Systems</td>
<td></td>
</tr>
<tr>
<td>Appendix VI</td>
<td>24</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----</td>
</tr>
<tr>
<td>Inadequate Resources to Accomplish IRM Goals</td>
<td></td>
</tr>
<tr>
<td>Appendix VII</td>
<td>26</td>
</tr>
<tr>
<td>Cost Overruns</td>
<td></td>
</tr>
<tr>
<td>Appendix VIII</td>
<td>28</td>
</tr>
<tr>
<td>Schedule Delays</td>
<td></td>
</tr>
<tr>
<td>Appendix IX</td>
<td>30</td>
</tr>
<tr>
<td>Information Systems Not Performing As Intended</td>
<td></td>
</tr>
<tr>
<td>Appendix X</td>
<td>32</td>
</tr>
<tr>
<td>Data That Were Inaccurate, Unreliable, or Incomplete</td>
<td></td>
</tr>
<tr>
<td>Appendix XI</td>
<td>34</td>
</tr>
<tr>
<td>Poorly Designed Systems Made Access to Data Time-consuming or Cumbersome</td>
<td></td>
</tr>
</tbody>
</table>
Appendix XII
Major Contributors to
This Report

Tables

Table 1.1: IRM Problems

Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADP</td>
<td>automated data processing</td>
</tr>
<tr>
<td>CFTC</td>
<td>Commodity Futures Trading Commission</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>EAGLE</td>
<td>Enhanced Automation for the Government Legal Environment</td>
</tr>
<tr>
<td>EEOC</td>
<td>Equal Employment Opportunity Commission</td>
</tr>
<tr>
<td>FAA</td>
<td>Federal Aviation Administration</td>
</tr>
<tr>
<td>FDA</td>
<td>Food and Drug Administration</td>
</tr>
<tr>
<td>FERS</td>
<td>Federal Employee Retirement System</td>
</tr>
<tr>
<td>GAO</td>
<td>General Accounting Office</td>
</tr>
<tr>
<td>HCFA</td>
<td>Health Care Financing Administration</td>
</tr>
<tr>
<td>IMTEC</td>
<td>Information Management and Technology Division</td>
</tr>
<tr>
<td>INS</td>
<td>Immigration and Naturalization Service</td>
</tr>
<tr>
<td>IRM</td>
<td>information resources management</td>
</tr>
<tr>
<td>IRS</td>
<td>Internal Revenue Service</td>
</tr>
<tr>
<td>LAMPS</td>
<td>Light Airborne Multipurpose System</td>
</tr>
<tr>
<td>MAISRC</td>
<td>Major Automated Information System Review Committee</td>
</tr>
<tr>
<td>NASA</td>
<td>National Aeronautics and Space Administration</td>
</tr>
<tr>
<td>NOAA</td>
<td>National Oceanic and Atmospheric Administration</td>
</tr>
<tr>
<td>NORAD</td>
<td>North American Aerospace Defense Command</td>
</tr>
<tr>
<td>OPM</td>
<td>Office of Personnel Management</td>
</tr>
<tr>
<td>SEC</td>
<td>Securities and Exchange Commission</td>
</tr>
<tr>
<td>SIDPER-3</td>
<td>Standard Installation/Division Personnel System III</td>
</tr>
<tr>
<td>SSA</td>
<td>Social Security Administration</td>
</tr>
<tr>
<td>SPAN</td>
<td>Space Physics Analysis Network</td>
</tr>
</tbody>
</table>
Our review of IMTEC's work performed from October 1988 to May 1991 identified 132 reports (out of a total of 192) that described IRM problems. We summarized these problems in ten categories; the table depicts the categories and the number of reports that fell within them each year.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Number of reports for fiscal year</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inadequate management of information systems development life cycle</td>
<td>24 33 9</td>
<td>66</td>
</tr>
<tr>
<td>Ineffective oversight and control of IRM</td>
<td>7 18 4</td>
<td>29</td>
</tr>
<tr>
<td>Inability to ensure the security, integrity, or reliability of information systems</td>
<td>3 11 2</td>
<td>16</td>
</tr>
<tr>
<td>Inability of systems to work together</td>
<td>2 8 4</td>
<td>14</td>
</tr>
<tr>
<td>Inadequate resources to accomplish IRM goals</td>
<td>2 5 2</td>
<td>9</td>
</tr>
<tr>
<td>Cost overruns</td>
<td>13 6 3</td>
<td>22</td>
</tr>
<tr>
<td>Schedule delays</td>
<td>10 8 2</td>
<td>20</td>
</tr>
<tr>
<td>Systems not performing as intended</td>
<td>3 3 1</td>
<td>7</td>
</tr>
<tr>
<td>Data that were inaccurate, unreliable, or incomplete</td>
<td>4 7 7</td>
<td>18</td>
</tr>
<tr>
<td>Systems that make access to data time-consuming or cumbersome</td>
<td>2 4 2</td>
<td>8</td>
</tr>
</tbody>
</table>

*Fiscal year 1991 reports include only those issued before May 31, 1991

*Reports that identified more than one problem are listed under more than one category, so the total number of reports is more than 132.
The information systems development life cycle refers to the development of a system from its conception to the point at which it is no longer used. It includes all of the activities associated with the analysis, acquisition, design, development, test, integration, operation, maintenance, and modification of a system. Government practice translates this life cycle into a series of discrete steps for managers to follow. Proper management includes steps such as analysis of user/organizational requirements to justify the system, periodic testing of the system during its development phase, and plans for monitoring the work load capacity of the system.

Careful management of the system development life cycle increases the likelihood that the system will perform as intended and will be delivered on time and within budget. Failure to effectively manage the development and modification of information systems was the most frequently reported source of problems. Sixty-six of our reports identified instances in which such management was inadequate. Problems ranged from not doing a proper cost/benefit analysis to inadequate testing of major system modules before the system became operational.

For example, failure to properly plan an information system’s development prompted us to question whether further development was warranted. A report on the Health Care Financing Administration (HCFA), part of the Department of Health and Human Services, stated that HCFA had not estimated total costs of a new Medicare claims processing system, did not document its expected benefits and savings, and did not test the system in a way that would generate useful information. The report recommended that the claims processing system—which at the time of the report had become operational—be discontinued if no benefit or cost savings could be proved.

Our reports also identified problems in the later stages of the systems development life cycle. One report questioned the adequacy of the Federal Aviation Administration’s (FAA) plan to replace antiquated computers in the Los Angeles basin area because the agency could not adequately judge whether the new computers would solve the major problem with the old system: insufficient computer capacity. A capacity management program—which FAA did not have—could assist in forecasting computer requirements to ensure that computers have sufficient capacity to meet peak demands. The report noted that without such a program, FAA had no

---

way to evaluate potential alternatives to both its short-term and long-term plans for the basin.

**Related Products**

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense Communications: Millions May Be Spent Unnecessarily to Expand Data Network (GAO/IMTEC-91-6, Nov. 7, 1990).</td>
</tr>
</tbody>
</table>


Appendix II
Inadequate Management of Information Systems Development Life Cycle


Coast Guard: Strategic Focus Needed to Improve Information Resources Management (GAO/IMTEC-90-32, Apr. 24, 1990).


Without oversight, an agency has no assurance that its system development projects are complying with the applicable standards, regulations, and management practices promulgated by an agency and by the government to reduce the chance of failure or delays. Numerous reports described oversight weaknesses in agencies' information management programs. For example, oversight problems at the Department of Defense were identified in a report that discussed Defense's Major Automated Information System Review Committee (MAISRC), which is responsible for reviewing the development efforts for any information system valued at over $100 million in total cost. One report noted that the Office of the Secretary of Defense was not terminating or redirecting development activity even when warranted by the results of MAISRC reviews.1

According to another report, the Immigration and Naturalization Service (INS) does not have readily available the information needed to identify, apprehend, and deport criminal aliens.2 This is due to missing data and to the inability of INS to share data among its own systems. This situation forces agency officials to query a number of different systems. In part, the problem of sharing information throughout INS was due to the agency's not providing adequate oversight of its IRM program. INS had not effectively evaluated its own management of information resources. Evaluations had focused on specific information systems, rather than addressing how effectively INS had managed its information resources as a whole.

A 1990 report identified inadequate controls within the Department of Education as allowing significant abuses in the Stafford Student Loan program.3 A total of $109 million in new loans was obtained by students who had defaulted on previous loans, and loans that totaled millions of dollars were disbursed to students who had reached their legal loan limits. These errors occurred because Education did not have adequate procedures for checking the accuracy and completeness of data in its loan data base and, therefore, was not able to identify student loan defaulters or determine the amount accrued by borrowers.


Appendix III
Ineffective Oversight and Control of Information Resources Management

Related Products


Customs Automation: Duties and Other Collections Vulnerable to Fraud and Abuse (GAO/IMTEC-90-29, Feb. 28, 1990).


Information Management: Issues Important to Farmers Home Administration Systems Modernization (GAO/IMTEC-89-64, Aug. 21, 1989).


Appendix III
Ineffective Oversight and Control of
Information Resources Management

Financial Integrity Act: Actions Needed to Correct ADP Internal Control
Weaknesses (GAO/IMTEC-89-11, May 9, 1989).
Appendix IV

Inability to Ensure Security, Integrity, or Reliability of Information Systems

Security of data is an important issue, both to the public and to the government. When agencies collect data, they must be able to ensure that the data are reliable and secure from unauthorized access. The reports included in this category identified problems ranging from unauthorized access to sensitive data to the inability to ensure the reliability or integrity of a system. Several reports stated that actual security breaches had occurred, either in the form of unauthorized access by individuals or computer viruses. Other reports noted agency weaknesses in evaluating potential risk to information systems that left them vulnerable to incursions or damage.

As an example of such an incursion, a report on the computer virus infection of several computers using Internet in 1988—including the Department of Energy's Lawrence Livermore Laboratory and the National Aeronautics and Space Administration's (NASA) Ames Research Center—demonstrated the vulnerability of both government and private-sector networks. Internet is the main computer network used by the United States research community. It includes over 500 networks, including ones sponsored by the National Science Foundation and the Department of Defense. Responsibility for computer security was handled primarily by the sites that own or operate the computers. The various networks making up Internet are the responsibility of the network's sponsor, such as a federal agency or a research consortium. The lack of a lead agency or organization responsible for network-wide security management created difficulties in responding to the virus. Problems communicating information about the virus to members of the network and in coordinating emergency response activities were reported. The amount of damage that could have been done to valuable scientific data is incalculable.

Another report showed that unauthorized users gained access dozens of times to NASA's Space Physics Analysis Network (SPAN), which assists scientists in conducting unclassified space-related research. At the time of the report, agency records showed that unauthorized access had taken place. NASA could not be sure that other incursions had not occurred undetected. Also, NASA could not judge the effectiveness of the security plans it had put in place to address the potential risks to SPAN because it had not performed a security risk analysis.

1Computer Security: Virus Highlights Need for Improved Internet Management (GAO/IMTEC-89-57, June 12, 1989).

Appendix IV
Inability to Ensure Security, Integrity, or Reliability of Information Systems

According to a 1990 report, the Department of Justice could not ensure the security of highly sensitive information, such as the names of defendants, witnesses, informants, and undercover law enforcement officials. Security weaknesses at Justice had heightened the possibility of unauthorized access to highly sensitive information or the interruption of computer services. For example, control of access to a sensitive data center was inadequate and software that could circumvent computer security safeguards was easily accessible. Also, contingency plans had not been prepared or had not been tested.

Related Products


Computer Security: Virus Highlights Need for Improved Internet Management (GAO/IMTEC-89-57, June 12, 1989).

The ability of systems within or among agencies to communicate and exchange data with each other enables agencies to more effectively perform their missions by sharing information. However, the inability of information systems to share data or work together has been a common problem throughout the federal government. This inability often results when systems are developed without considering interagency or even agencywide needs. In some cases, a lack of planning, problems implementing plans, and changes to requirements have contributed to the problem.

A classic example was discussed in a 1990 report, which stated that the Veterans Administration's (now Department of Veterans Affairs) systems were incompatible and could not readily exchange data within the agency and with external agencies, such as the Department of Defense. To illustrate, the report showed that the Veterans Administration had to wait an average of 2 months to obtain Defense records documenting military service. Because of the delay in receiving records from Defense as well as other problems such as the Veterans Administration's paper-intensive, manual processing system, it was not unusual for a veteran to have to wait over 150 days for a claim to be processed.

Another 1990 report noted that the Army was not able to ensure that its new information systems could share data and work together because it had not completely implemented its IRM program. Specifically, it had not completed development of an Army-wide information system architecture to provide implementation guidance and milestones for the development of new systems. Instead, Army components were developing information systems without any guarantee that the systems would be able to share data and work together.

A recent report highlighted the interoperability problems that the law enforcement community faces in managing the war on drugs. A vital intelligence center for the Coast Guard's law enforcement activity used a system that could not accept data electronically from another system. As a result, Coast Guard personnel had to manually enter large amounts of drug intelligence data into the system. Coast Guard officials acknowledged that valuable time and resources were wasted because of this manual process.

---

Appendix V
Inability of Systems to Work Together

Related Products


Defense Communications: Millions May Be Spent Unnecessarily to Expand Data Network (GAO/IMTEC-91-6, Nov. 7, 1990).


Coast Guard: Strategic Focus Needed to Improve Information Resources Management (GAO/IMTEC-90-32, Apr. 24, 1990).


Agencies have cited a lack of resources as an impediment to fulfilling IRM goals. Identified constraints included too few technical personnel and budget shortfalls. The most reported problem in this category was a lack of technical expertise.

The Navy believed a limited pool of skilled Ada programmers could cause schedule delays in the development of its new target detection software, according to a 1989 report. The Navy had set an ambitious development schedule in order to have the system on hand for integration with its new Seawolf submarine. The schedule, however, was dependent on experienced Ada programmers. At the time of the report, the contractor developing the software did not have a consistent training program in place for Ada programmers. The report warned of the potential for reduced programmer performance, an increased number of coding errors, or both.

The Internal Revenue Service (IRS) faced a funding deficit in 1989 and 1990 for its ADP conversion of payroll and personnel systems. IRS was not sure it could complete its conversion on schedule or adequately train its payroll and personnel staff on the new system given its constrained budget. One official involved in the conversion process was concerned that if the conversion schedule slipped, costs could be greatly increased in performing the conversion.

Related Products


---

1Ada is the standard programming language for the Department of Defense.


Appendix VI
Inadequate Resources to Accomplish IRM Goals


Cost overruns were significant in many of the federal government's information system development efforts we examined. Cost overruns totalling over $7 billion were identified. For example, a 1989 report stated that an IRS system being developed to automate the examination of tax returns had experienced a rise in cost estimates of $800 million. In May 1985, the system was expected to cost $1 billion over the life of the system. IRS' 1988 prediction was that the system would cost $1.8 billion.

In another example, the Air Force had been attempting to modernize the computer systems resident in the North American Aerospace Defense Command's (NORAD) Cheyenne Mountain complex since 1981. As of 1989, the Air Force had estimated it would need an additional $535 million to complete the modernization.

Related Products

**Space Data:** NASA's Future Data Volumes Create Formidable Challenges (GAO/IMTEC-91-24, Apr. 8, 1991).


**Air Traffic Control:** Efforts to Modernize Oceanic System Delayed (GAO/IMTEC-91-2, Jan. 16, 1991).


**ADP Budget:** Potential Reductions to the Department of Defense's Budget Request (GAO/IMTEC-90-12, Jan. 10, 1990).


Appendix VII
Cost Overruns


Air Traffic Control: Voice Communications System Continues to Encounter Difficulties (GAO/IMTEC-89-39, June 1, 1989).


ADP Acquisition: Navy's Efforts to Develop an Integrated Disbursing and Accounting System (GAO/IMTEC-89-20FS, Feb. 8, 1989).


Schedule delays were significant in many of the federal government's information system development efforts. For example, one report stated that by 1994 the Navy, in its own best estimate, will have spent 17 years developing a system to automate a manual process of preparing and editing data-entry documents for a centralized payroll and personnel system.\(^1\) The system, started in 1977, was to have been operational by 1982. As of February 1990, however, information on only 64 percent of active-duty personnel had been entered into the system. According to the Navy, the system was not expected to be fully operational until 1994, which would make it 12 years overdue.

Another example of schedule problems in systems development involved a new voice communications system being developed by FAA. Implementation of the system was delayed 6 years.\(^2\) The schedule delays occurred in part because FAA and its contractors underestimated the complexity of building the system.

### Related Products


\(^2\)Air Traffic Control: Voice Communications System Continues to Encounter Difficulties (GAO/IMTEC-89-39, June 1, 1989).


ADP Budget: Potential Reductions to the Department of the Navy's Budget Request (GAO/IMTEC-89-75BR, Sept. 18, 1989).


Air Traffic Control: Voice Communications System Continues to Encounter Difficulties (GAO/IMTEC-89-39, June 1, 1989).


Information systems used in daily agency operations have failed to perform the tasks for which they were intended. One example of this problem was the difficulty IRS had with its interim electronic filing system during the 1988 tax filing season.\(^1\) An essential component of IRS' system was the imaging subsystem, which permitted tax examiners to access and annotate images of tax returns, rather than relying on paper originals and copies. When the imaging subsystem did not work, IRS tax examiners had to use stopgap measures such as printing paper copies of the returns, annotating their corrections, and storing these paper records.

In another example, a 1989 report documented that the Air Force was still having critical operational and performance problems with its new satellite communications system.\(^2\) Because of the problems with the computer hardware and software, the new system was only able to handle 55 percent of the communications required between the military satellites and ground facilities. The report concluded that until technical deficiencies were resolved, the planned deactivation of an older system that was expensive to maintain would be delayed.

### Related Products

- **Military Space Operations:** Operational Problems Continue With the Satellite Control Computer System (GAO/IMTEC-89-56, Aug. 8, 1989).
- **Air Traffic Control:** Voice Communications System Continues to Encounter Difficulties (GAO/IMTEC-89-39, June 1, 1989).


Appendix IX
Information Systems Not Performing As Intended

Data That Were Inaccurate, Unreliable, or Incomplete

Numerous examples of inaccurate, unreliable, or incomplete data were discovered. One report found that the Veterans Administration had not been able to easily maintain the quality of its information because its data resided in over 150 fragmented automated systems and multiple, ad hoc manual systems. Consequently, the Veterans Administration could not verify the quality of the service it provided to veterans.

In another report, NASA was criticized for not storing any data for some missions and having incomplete data for many important missions. For example, the data collected by the Apollo 9 mission in 1969 had not been stored in a NASA facility and its current location was unknown at the time of the report. For those missions for which NASA had stored data, agency policy only required the archiving of analyzed data, and not the data from which the analysis was derived. Once analyzed, the original data were destroyed. Both NASA's own and other studies have shown the value of retaining original data sets for the use of future researchers.

Related Products

Medicare: Flawed Data Add Millions to Teaching Hospital Payments (GAO/IMTEC-91-31, June 4, 1991).


Appendix Y
Data That Were Inaccurate, Unreliable, or Incomplete


Coast Guard: Strategic Focus Needed to Improve Information Resources Management (GAO/IMTEC-90-32, Apr. 24, 1990).

Customs Automation: Duties and Other Collections Vulnerable to Fraud and Abuse (GAO/IMTEC-90-29, Feb. 28, 1990).


Tax System Modernization: IRS' Efforts to Improve Taxpayer Correspondence (GAO/IMTEC-90-26, Mar. 22, 1990).


Appendix XI

Poorly Designed Systems Made Access to Data Time-consuming or Cumbersome

Instances in which agencies' poorly designed or implemented systems made data access difficult were identified. The access problems ranged from an inconvenience or time delay in obtaining information to information being so difficult to retrieve that agency personnel rarely use it.

For example, a 1989 report stated that the Social Security Administration's field offices did not have easy access to information required to process retirement claims. Among other problems, they had to use two different systems to get the information, which caused user dissatisfaction and minor delays in getting needed information. Another report documented that the Coast Guard field office staff found its major law enforcement system so difficult, tedious, and time-consuming to use that staff rarely used the system to support decisions.

Related Products


## Major Contributors to This Report

| Information Management and Technology Division, Washington, D.C. | Nancy A. Simmons, Assistant Director |
| | Suzanne M. Burns, Assignment Manager |
| | Kevin G. McCarthy, Evaluator-in-Charge |
| | Alicia D. Wright, Computer Scientist |
Ordering Information

The first copy of each GAO report is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20877

Orders may also be placed by calling (202) 275-6241.