United States General Accounting Office

GAO

Report to the Chairman, Committee on Veterans' Affairs, House of Representatives

July 1987

HOSPITAL ADP SYSTEMS

VA Needs to Better Manage Its Decentralized System Before Expansion

C39765
133745

GAO/IMTEC-87-28

GAO

United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

B-223388

July 24, 1987

The Honorable G. V. (Sonny) Montgomery
Chairman, Committee on Veterans' Affairs
House of Representatives

Dear Mr. Chairman:

This report responds to your request that we evaluate the Veterans Administration's (VA) Decentralized Hospital Computer Program and the demonstration test of three commercial systems. We identified ways to improve the decentralized system, discussed factors that need consideration during system expansion, and addressed the test of commercial systems in VA.

The report makes recommendations to the Administrator of Veterans Affairs for improving the management of the program. The report also cites a matter for congressional consideration concerning VA's medical computerization needs.

As arranged with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution of the report until 15 days from its issue date. At that time, we will send copies to the Chairmen, Senate and House Committees on Appropriations; the Chairman, Senate Committee on Veterans' Affairs; the Chairman, Senate Committee on Governmental Affairs; the Chairman, House Committee on Government Operations; the Director, Office of Management and Budget; interested congressional committees; and other interested parties. Copies will also be made available to others upon request.

Sincerely,

Ralph V. Carlone

Ralph V. Carlone
Director

Executive Summary

Purpose

The Veterans Administration (VA) is the largest provider of medical services in the nation. To facilitate handling the large amounts of data generated by the services provided at its 172 medical centers and to improve service to veterans, VA began installing the Decentralized Hospital Computer Program in 1983.

Because of the importance of the agency's computerization efforts, the House Committee on Veterans' Affairs asked the General Accounting Office (GAO) to provide an analysis of

- the status of VA's decentralized system;
- VA's effectiveness in managing the development and implementation of its decentralized system, including the adequacy of its cost and benefit analyses; and
- VA's demonstration test of three commercial systems as alternatives to the decentralized system.

Background

Since the mid 1960's, VA has sought to improve medical service to veterans by developing and implementing computer systems for its medical centers. The limited success of these early attempts led to implementation of VA's decentralized system. The agency's goal is to develop a system consisting of separate software units (known as modules) that will automate and integrate medical center information for such functions as hospital admissions, pharmacy and laboratory operations, and patient care. Some of this information will ultimately be used by management agencywide.

In 1983, the planned system had 11 modules with an estimated 7-year-life-cycle cost of $155 million in 1983 dollars. By 1986, VA had expanded the planned system to include 51 modules with an estimated 19-year-life-cycle cost of $1.2 billion in 1986 dollars. In June 1987, VA reduced the scope of the system to 14 modules with an estimated 10-year-life-cycle cost of $925 million in 1987 dollars.

While funding development of the decentralized system, the House and Senate Appropriations Committees also directed VA in 1983 to test commercial hospital computer systems to determine if they would be more cost-effective than the agency's system. VA anticipates completion of its $22.6 million test of commercial systems in three medical centers in September 1987.

Results in Brief

Users GAO interviewed indicated that the initial phase of VA's decentralized system was meeting their most critical needs and was helping to improve service to veterans. However, GAO found some shortcomings in the system. It did not adequately safeguard patient records from inaccurate data entry, unauthorized changes, or destruction, and permitted the creation of multiple patient records. Such shortcomings existed largely because the office responsible for managing the project did not have authority to ensure that sound practices were used in all aspects of the system's development and implementation. In recent months VA has recognized these problems and initiated corrective actions, including providing the management office greater authority over the program.

VA is planning to embark on a multi-million dollar expansion of the system without an adequate analysis to determine the most cost-effective approach. The Federal Information Resources Management Regulation requires agencies to consider the operational and economic feasibility of alternatives before acquiring automatic data processing capabilities. GAO found, however, that VA did not adequately explore the potential for less costly system alternatives than the decentralized system approach it had selected.

The test of three commercial systems does not provide an appropriate basis for comparison with the VA system. Nevertheless, on the basis of a consultant's analysis, the agency believes the commercial systems are too expensive and are not a viable alternative to the decentralized system.

Principal Findings

Users Satisfied With Current System but Problems Exist

Between 1983 and January 1987, VA spent about $200 million installing six Core modules—those that it considers the foundation of its decentralized system—at 169 medical centers. GAO's interviews with 252 users at 13 medical centers indicated that, in general, they believed that the system met their needs for critical information, was accurate and easy to use, helped them do their jobs better, and provided the flexibility needed in a computer system.

Over the next 10 years, VA plans to spend about $925 million to support and expand the system. These plans involve supplementing the Core modules with eight Enhanced modules. Most of the additional modules

will computerize more functions for medical centers, while others will provide regional offices and headquarters with agencywide management information. Three of the Enhanced modules were developed, but not installed, as of January 1987.

Although users believed the installed system was performing satisfactorily and meeting their most critical needs, it had some shortcomings. First, the software did not include control features that could help prevent creating multiple patient records or making unauthorized changes to the records. Second, software was released before it was appropriately tested, documented, and approved, thereby causing numerous software revisions. Finally, the agency did not establish adequate internal controls to safeguard patient data from theft, unauthorized disclosure, or alteration, and it did little to limit risks to the decentralized system from natural disasters

These problems could have been avoided or been less severe if VA had provided adequate central management control over the development and implementation of the system. Although VA established the Medical Information Resources Management Office to be responsible for managing the system, it did not provide the office with the authority it needed to ensure that sound practices were followed at the local level in planning, developing, implementing, and maintaining the system.

In February 1987, VA made organizational changes to provide the office with authority to better manage the system. The agency has also initiated actions to correct system shortcomings. (See pp. 18-35.)

Better Cost and Benefit Information Needed for Informed Decision Making

GAO believes that the Congress and VA would be in a better position to make upcoming decisions concerning the direction of the agency's planned system expansion if VA had developed a comprehensive life-cycle cost estimate and cost/benefit analysis that included an assessment of alternatives. Federal regulations and guidelines require these estimates and analyses and describe what they should include.

GAO found that VA had omitted costs for items such as telecommunications, utilities, and supplies in its earlier life-cycle and cost/benefit analyses. In responding to a draft of this report, VA noted that it had reduced the scope of the decentralized system and included estimates for the omitted items GAO had identified. Although these analyses are more complete, without considering feasible hardware alternatives, VA cannot be assured that it has selected the most cost-effective approach. For

example, a regionalized approach—using one computer to support several medical centers rather than placing a computer in each of VA's 172 medical centers—may substantially reduce hardware, facility, and personnel costs. (See pp. 36-49.)

Commercial Test Structure Is Inappropriate

The three commercial systems VA is testing offer features similar to those of the decentralized system, and users are generally satisfied with the services they provide. However, VA did not structure the test to provide a direct basis for determining whether the commercial systems could meet the same requirements as the decentralized system in a more cost-effective manner.

The vendors were permitted to modify their systems to meet local test sites' requirements. As a result, these requirements were not comparable to VA's system requirements. Also, each vendor's test contract included a fixed-cost option for installing its system at medical centers that were only one of the following sizes: small, medium, or large. While the sum of the contracts' options is $2.1 billion in 1984 dollars for a 7-year life cycle, vendors claim the commercial-system costs could be reduced if they were permitted to propose costs for installing their system at all sizes of medical centers, thus allowing them to fully consider economies of scale when developing their proposed costs.

Notwithstanding the shortcomings of the test, VA has concluded that the commercial systems can be compared to the decentralized system by making several assumptions and that they are too expensive for further consideration. While VA did not plan to expand the use of the commercial systems, it had no specific plans to phase them out before fiscal year 1989. (See pp. 50-57.)

Recommendations

This report contains a number of recommendations to improve system development and implementation practices. (See pp. 59-60.) In a draft of this report, GAO recommended that VA develop a life-cycle cost estimate and a cost/benefit analysis that consider various system design alternatives including a commercial system approach. GAO suggested that the Congress consider limiting VA funding pending satisfactory completion of the life-cycle cost estimate and cost/benefit analysis.

Agency Comments and Our Evaluation

In commenting on the draft report, VA agreed that GAO had identified a number of significant problems related to system development and implementation and said that, in general, it had already noted and moved to resolve them. However, the agency did not concur with GAO's position on the need for further consideration of design alternatives. VA stated it had selected a decentralized approach rather than other alternatives, such as a regionalized approach, because a decentralized approach is needed to meet critical aspects of its information management program and allow hospital managers to have adequate control over and responsibility for their systems.

VA also indicated that taking time to explicitly evaluate other alternatives would delay and thereby adversely affect its computerization effort and ultimately its service to veterans. It concluded that a regionalized system alternative had been "implicitly evaluated and determined not to be cost-effective," particularly because of increased telecommunications costs. The agency added that its consultant's study had found the commercial systems being tested were significantly more costly than the decentralized system. However, the consultant's study of commercial systems did not include consideration of system design alternatives, and VA did not perform a detailed analysis to support its conclusion regarding the use of a regionalized approach within its decentralized system. (See pp. 60-61.)

Matter for Congressional Consideration

GAO believes that now, before VA initiates a major investment to enhance its decentralized system, is an opportune time to assess the feasibility of potential system design alternatives. However, VA believes that a decentralized configuration is needed to meet its local management and control objectives and that the consideration of other alternatives could adversely affect service to veterans. The Congress must ultimately decide whether the issues raised by VA justify its not explicitly considering potentially more cost-effective system design alternatives in meeting VA's medical computerization needs. GAO believes the information in this report should assist the Congress in reaching future funding decisions on this program. (See p. 62.)

Contents

Executive Summary		2
Chapter 1 Introduction		10
	VA's Medical Work Load Is Increasing	10
	Earlier Efforts to Computerize VA Hospitals	11
	VA's Decentralized Hospital Computer Program	11
	VA's Integrated Hospital System Project	15
	Objectives, Scope, and Methodology	15
Chapter 2 Operational DHCP Satisfies Users but Has Some Shortcomings		18
	Users Are Satisfied With Implemented Functions and System Operations	18
	Shortcomings of Initial Implementation Could Affect Patient Care	21
Chapter 3 DHCP Expansion Planned Without Information Necessary for Informed Decisions		36
	Expansion Plans Include Substantial Amounts of Software, Hardware, and Telecommunications	36
	Latest Cost/Benefit Analysis Did Not Include Consideration of Hardware Configuration Alternatives	37
	System Utilization and Capacity Statistics Not Being Obtained for Planned Procurement	46
	Central Management Not Ensuring Consensus on Key Data in Order Entry/Results Reporting Feature	48
Chapter 4 Commercial Systems' Test Not Appropriately Structured to Compare Costs and Benefits		50
	Commercial Systems and DHCP Have Similar Basic Computer Functions and Levels of User Satisfaction	50
	Test Structure Prevents Direct Comparison Between Commercial Test Systems and DHCP	51
	Under Contract Limitations, Commercial Test Systems Offer Fewer Features and Cost More Than DHCP	52
Chapter 5 Conclusions, Recommendations, and Agency Comments and Our Evaluation		58
	Conclusions	58
	Recommendations	59
	Agency Comments and Our Evaluation	60
	Matter for Congressional Consideration	62

Appendixes

Appendix I: Description of VA's DHCP Initial and Full Core Modules 64
Appendix II: Development Status of Currently Planned DHCP Enhanced Modules 66
Appendix III: Previously Planned Enhanced and Comprehensive Modules That Now Are Not Included in the DHCP System 67
Appendix IV: Criteria for Developing Full Cost Estimates 69
Appendix V: Commercial-System Users Interviewed Were Satisfied With Vendor Systems 72
Appendix VI: Agency Comments 73

Tables

Table 4.1: Commercial-System Test Sites Generally Met Information Needs of Users Interviewed 51

Figures

Figure 1.1: Changes to VA's Decentralized System and Life-Cycle Cost Estimates 13
Figure 1.2: Core Modules Supporting VA Medical Services in a Medical Center and an Outpatient Clinic 14
Figure 2.1: DHCP Core Software Generally Met Informational Needs of the Users Interviewed 19
Figure 2.2: Users Interviewed Were Satisfied With DHCP System 20
Figure 3.1: VA's Decentralized System and Life-Cycle Cost Estimates (By Fiscal Year) 40
Figure 4.1: DHCP Compared to Commercial Systems 53

Abbreviations

ADP	automatic data processing
DHCP	Decentralized Hospital Computer Program
GAO	General Accounting Office
MAS	Medical Administration Service
VA	Veterans Administration
VAMC	Veterans Administration Medical Centers

Introduction

A key objective of the Veterans Administration (VA) is to provide timely, high-quality medical care to all eligible veterans. To meet this goal, VA operates the largest civilian health care system in the United States serving millions of veterans with medical, surgical, and psychiatric care. The scope of VA's health care system, according to agency officials, requires that the agency have modern computer capabilities to meet critical information needs and thereby improve patient care. From the mid-1960's until the early 1980's, VA had difficulties in successfully acquiring and operating automated systems in support of its medical centers. Since 1983, the agency has been computerizing its medical centers under the Decentralized Hospital Computer Program (DHCP), whose software was developed by VA employees. The agency has also been testing commercially developed systems in three medical centers under the Integrated Hospital System project.

VA's Medical Work Load Is Increasing

VA provides medical care at 172 hospitals, 227 outpatient clinics, 115 nursing homes, and 16 domiciliaries (dwellings where minimum medical care and living space are provided for veterans). Any hospital or a combination of a hospital and one or more of the other facilities is referred to as a medical center. These medical centers, which are geographically dispersed in seven VA regions across the United States, range in size from 80 to 1,300 beds, and provide inpatient and outpatient care. Annual outpatient visits to the centers vary between 2,500 and 320,000 per site. The agency's medical facilities are staffed by about 202,000 employees, and its health care system, which had a 1986 annual budget of approximately $9.5 billion, generates an increasing volume of patient and administrative data. During 1986, for example, VA needed to maintain data on its health care delivery related to

- 1.3 million inpatient hospitalizations (73,000 average daily inpatients),
- 18.5 million outpatient clinic visits,
- 52 million prescriptions, and
- 183 million laboratory procedures.

From 1977 through 1986, the number of inpatient hospitalizations increased by 8 percent, and the number of outpatient clinic visits increased by 26 percent.

Earlier Efforts to Computerize VA Hospitals

From the mid-1960's until the early 1980's, VA procured numerous computer systems for its medical centers. However, these systems were not standardized to meet similar data needs VA-wide, nor were they centrally procured. In reporting[1] on the agency's management and use of its computer systems, we noted, among other things, that (1) the sharing of successful systems was not systematically pursued, (2) coordination of computer usage was hindered by the hospitals' traditional autonomy as well as the absence of any formal process for accountability, (3) the computer planning process lacked consideration of the interdependent need for data among the medical services, and (4) VA had not involved computer system users in the requirements definition, design, and development phases.

VA's Decentralized Hospital Computer Program

Recognizing the existence of serious information resources management problems, the VA Administrator, in October 1981, directed an analysis and reexamination of the agency's overall automatic data processing (ADP) plans and programs. A 1982 VA Executive Order established DHCP and sanctioned computer decentralization in the medical centers. This decentralized program involved using computers at each medical center to process local medical data. VA's Department of Medicine and Surgery—headed by the Chief Medical Director—was assigned primary responsibility for the program.

VA's goal in DHCP was to develop a totally integrated[2] medical center information system built around a local data base of patient and administrative information. The data base in each medical center is planned to support local management, as well as meet agencywide management needs through aggregation of data to regional and headquarters levels.

VA began developing DHCP in 1982 and procuring the computer hardware in 1983. Through this program, 169 medical centers, which include a total of 225 facilities, received initial system modules for both patient and administrative data during 1984 and 1985. A module represents a software application necessary to computerize a particular function. For example, the patient registration module computerizes key information necessary to register a patient and provides applicable demographic

[1] VA Must Strengthen Management of ADP Resources to Serve Veterans' Needs (GAO/FGMSD-80-60, July 16, 1980)

[2] VA uses the term integrated to describe a computer system (hardware and software) that uses common file structures, data files, system utilities, and user interfaces and links information processing functions, such as patient care, administrative operations, and management support. An integrated data base links the data originating from multiple sources and different software programs.

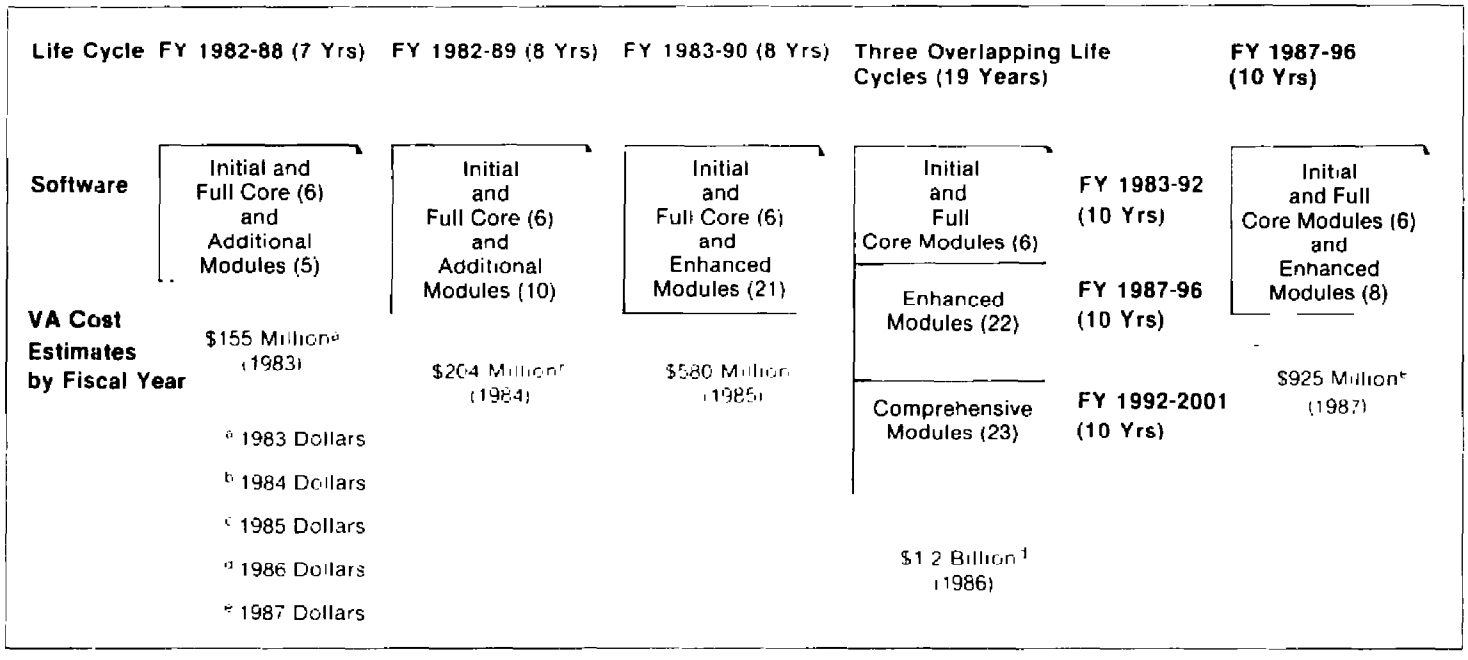
information to system users. VA is incrementally developing modules using a prototyping approach. Under this approach, selected system users review working models of modules early in their development. Software developers and system users then discuss the modules' requirements, and necessary changes are made as the system is further refined

During each of the past 3 years, VA expanded its planned system by extending the estimated life of the system and adding modules. In February 1987, the planned system consisted of 6 Initial and Full Core, 22 Enhanced, and 23 Comprehensive modules covering a 19-year life cycle (in three, 10-year, overlapping life cycles) at an estimated total cost of $1.2 billion in 1986 dollars.[1] In a June 5, 1987, response to our draft report, VA stated that the scope of DHCP had been revised to limit the program to those applications that have been shown to have a net benefit over their life cycles. The agency added that DHCP is currently limited to the six Initial and Full Core modules plus eight approved Enhanced modules. VA stated that the current DHCP covers a 10-year life cycle beginning in fiscal year 1987 at an estimated total cost of $925 million (using a 34.35-percent fringe benefit rate to reflect the federal government's full share of retirement costs). According to VA, the remaining 14 Enhanced and 23 Comprehensive modules in the 1986 estimates are now only potential areas for future automation, which will be added to the system only if their costs are considered to be justified and the modules approved by the Office of Management and Budget. (Figure 1.1 shows how the life-cycle costs have changed over the years.)

The Core software is the foundation of each medical center's system. The Initial Core modules are: patient registration, clinic scheduling, admission/discharge/transfer, and outpatient pharmacy. The Full Core modules include the Initial Core modules plus inpatient pharmacy and laboratory modules. The eight approved Enhanced modules are: radiology, dietetics, medical records tracking, integrated funds control/control point activity/accounting and procurement, surgery, decentralized medical management system, nursing, and mental health. A typical medical center computer system has the Core module data on each patient stored in its data base. The Core modules' data are entered at each service area. The data immediately become available to any authorized medical center staff through the integrated data base that links data entered

[1] All of VA's life-cycle cost estimates are in constant, undiscounted dollars. Discounting is a standard practice by which expected future cash flows are estimated and reduced to reflect the time value of money.

Figure 1.1: Changes to VA's Decentralized System and Life-Cycle Cost Estimates



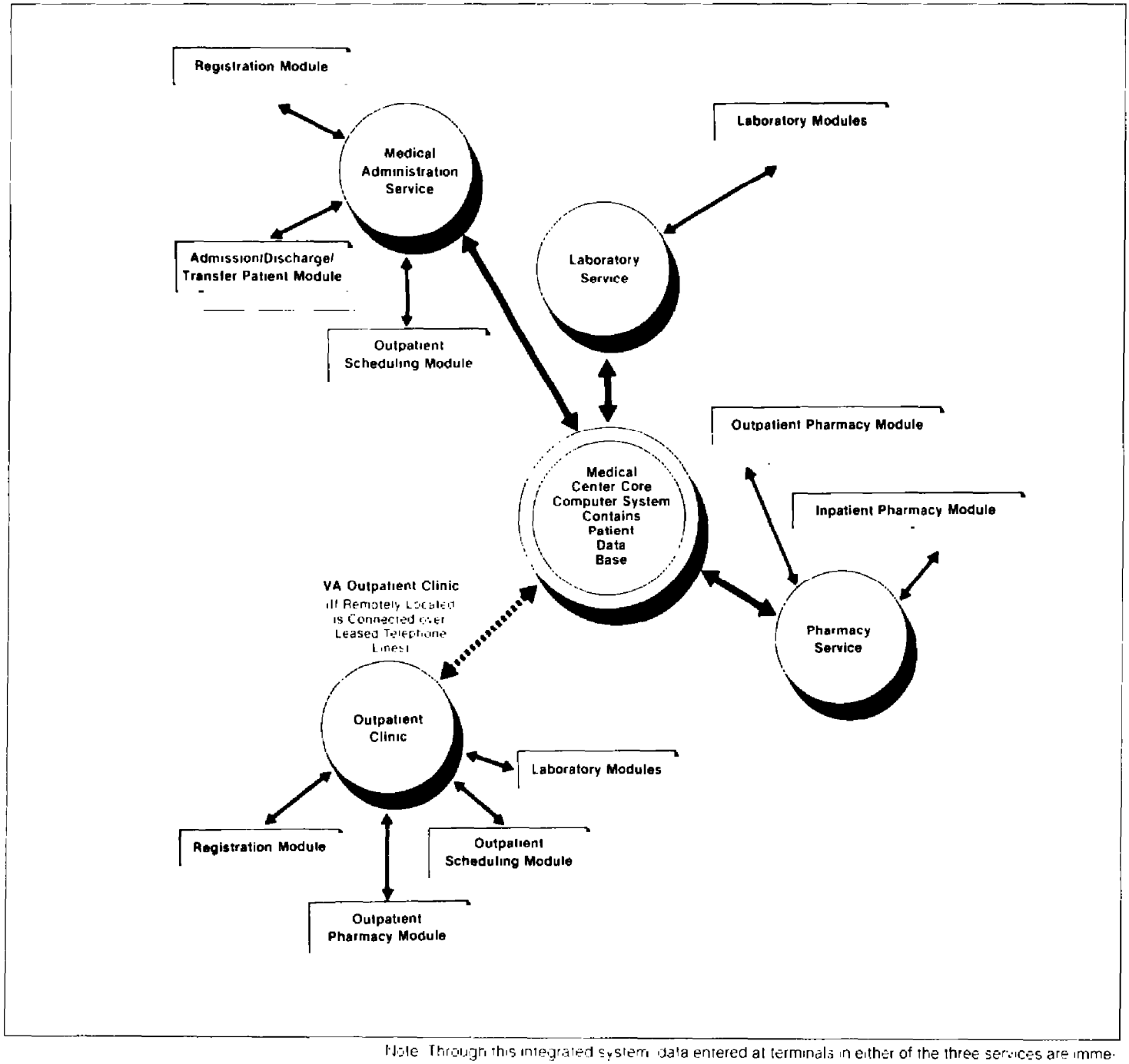
from different modules. For example, a nurse or physician can obtain laboratory test results on a patient at a nurses' station computer terminal as soon as these results are entered into the data base by the Laboratory Service staff. Figure 1.2 illustrates how the Core modules are used in medical centers and outpatient clinics.

In addition to the services provided by the Initial and Full Core modules, the eight Enhanced modules will provide essential computer support to the various local medical services as well as to regional and headquarters management. One of the top-priority Enhanced modules is the Decentralized Medical Management System module that VA plans to use to consolidate medical and financial data for use by local, regional, and headquarters management. A VA official said the agency plans to use this module to respond to a GAO report[4] that recommended that such data be collected for management decision making.

VA determined the Initial and Full Core modules to be the critical software needed in its medical facilities, and placed a high priority on installing them at individual locations. By January 1987, the Initial Core

[4]Financial Management: An Assessment of the Veterans Administration's Major Processes (GAO/AFMD-86-7, June 1986).

Figure 1.2: Core Modules Supporting VA Medical Services in a Medical Center and an Outpatient Clinic



Note: Through this integrated system, data entered at terminals in either of the three services are immediately available to all authorized system users through the common patient data base.

modules were operating in 169 VA medical centers, and the Full Core modules were at least partially operating in all but 17 of these centers. In addition, seven Enhanced modules have been developed and are available for implementation. Although, as of May 1987, five Comprehensive modules were under development or testing, these modules are no longer considered part of the DHCP system. (See appendix I for a description of the Initial and Full Core modules, appendix II for the development status of the currently planned Enhanced modules, and appendix III for information on previously planned Enhanced and Comprehensive modules.)

VA's Integrated Hospital System Project

In 1980 the Appropriations Conference Committee directed VA to determine whether commercial computer systems or VA's system would be the "most cost-effective and of maximum value" to the agency's vast medical center work. Before installing systems agencywide, VA was to analyze various alternatives using suitable test and validation methods to determine appropriate functional and integrated capabilities needed throughout VA's hospitals. In 1983, the House and Senate Appropriations Committees directed VA to conduct tests of commercially available medical information systems at three medical centers of varying sizes. The Congress appropriated funds in the fiscal year 1984 Appropriations Act to begin these tests.

Under the Integrated Hospital System project, which is also administered by the Department of Medicine and Surgery, contracts totaling $22.6 million were awarded to three vendors in August 1984 to test their commercial systems at three medical centers. The vendors were asked to consider optional software and were required to install certain mandatory programs and modify them to support medical center activities. VA plans to operate these commercial systems through the end of the demonstration test period in September 1987.

Objectives, Scope, and Methodology

The Chairman, House Committee on Veterans' Affairs, asked us to review the status and management of the DHCP system and the commercial systems test. In subsequent discussions with the Committee, it was agreed that we would determine

- the status of DHCP and whether this program addresses VA's medical center information needs,

- whether VA's approach to implementing and managing DHCP meets user needs and adequately addresses internal controls and cost/benefit analyses, and
- whether the demonstration test of the Integrated Hospital Systems provides a direct basis for comparing them with DHCP.

To determine the status of DHCP, we had headquarters officials identify the modules by the following categories: implemented throughout the agency, available but not fully implemented, being tested, under development, or not under development. We also had the officials identify the implementation schedule for the modules under development. To determine how DHCP was developed and whether it was meeting VA's needs, we judgmentally selected and visited 13 medical centers with DHCP's system in operation. These sites represented the operations of at least two medical centers in each of six VA geographical regions and in all five sizes of computer sites. The sites visited were Albany, N.Y.; Albuquerque, N.Mex.; Birmingham, Ala.; Fayetteville, N.C.; Grand Junction, Colo.; Hines, Ill.; Long Beach, Calif.; Manchester, N.H.; Martinez, Calif.; St. Cloud, Minn.; Seattle, Wash.; Tampa, Fla.; and Washington, D.C. We also visited the three medical centers in the commercial systems' test. These sites were Big Spring, Tex.; Philadelphia, Pa.; and Saginaw, Mich. From November 1985 through February 1986, we used structured interviews to obtain information on the sites' system implementation, operation, software, and internal controls. We judgmentally selected and interviewed 31 management officials at VA's six[1] regional Information Systems Centers, 96 management officials and 252 system users at 13 DHCP sites, as well as 85 individuals at the three commercial system sites.

We visited VA's Information Systems Centers to interview officials on procedures for developing software, verifying and testing software, and providing technical support to the medical centers in their regions. These sites were Albany, N.Y.; Birmingham, Ala.; Hines, Ill.; Salt Lake City, Utah; San Francisco, Calif.; and Washington, D.C.

To determine whether VA was following accepted guidelines and procedures in managing and operating DHCP, we reviewed federal guidelines for computer resources management and costing, and literature on computerization of medical facilities. We also interviewed officials from VA headquarters, the Office of Management and Budget, and the General

[1]A seventh Information Systems Center was established in 1986 to serve VA's newly formed seventh regional office area. These centers were originally known as Verification and Development Centers.

Services Administration to obtain information on the system's implementation, operation, software development, life-cycle costs, and delegation of procurement authority.

To assess the internal controls and determine the potential risks to system reliability and effectiveness, we reviewed, analyzed, and tested the controls at each of the 13 medical centers, and tested for multiple records at San Francisco, Calif , and Birmingham, Ala. We compared our findings with federal guidelines related to general and application internal controls, including Office of Management and Budget Circulars A-71 and A-130, applicable Federal Information Processing Standards Publications, and VA's policies on software and security.

To determine whether VA's estimated life-cycle costs of DHCP were adequate, we assessed the agency's February 1985 life-cycle cost submission to the Office of Management and Budget of $580 million and its February 1986 life-cycle cost estimate of $1.2 billion. We compared reported cost categories with federal guidance on computer system costs, interviewed VA officials responsible for developing the life-cycle cost estimates, and spoke to other VA officials with knowledge of specific cost categories and staffing requirements. Although we did not assess in detail VA's current 10-year, life-cycle cost estimate of $925 million, we verified that VA had included in this estimate those cost categories that we had noted missing in VA's 1986 estimate.

To determine whether the commercial systems demonstration test was appropriately implemented to compare with DHCP, we analyzed the (1) software functions available and planned in the DHCP and commercial systems, (2) systems' operations and user satisfaction, (3) estimated life-cycle costs of the systems, and (4) vendors' contracts. We interviewed VA software developers and vendor representatives about their current and planned software development using a preformatted listing of 1,483 hospital system functions that were judged applicable to VA. Because of time constraints, we did not verify that the reported items were either operational or planned as indicated by the respondents.

We conducted our review from November 1984 to June 1986 in accordance with generally accepted government auditing standards. Between June 1986 and June 1987, we periodically contacted VA to update our data.

Operational DHCP Satisfies Users but Has Some Shortcomings

Managers and users we interviewed were generally satisfied with the initial phase of DHCP, installed during 1983 through 1986, and said they believed the system provided information needed to improve service to veterans. VA's decentralized approach to developing and installing the system seems to have been a major contribution to the agency's success in meeting users' critical needs in a short period. Under this approach, VA's Medical Information Resources Management Office at headquarters provided general guidance that allowed VA software developers in the regions to independently develop modules for agencywide implementation. However, because the agency did not give its Management Office the authority needed to ensure that DHCP was effectively implemented, the system has some shortcomings. The shortcomings—which relate to software development and internal controls over computer facilities and patient data—increase the risk of inaccuracies in, and unauthorized access to, patient data and VA's inability to operate computer facilities after natural disasters. These conditions could affect patient care. VA has recognized most of the problems and has begun taking corrective actions.

Users Are Satisfied With Implemented Functions and System Operations

Most of the 348 managers and users we interviewed[1] at 13 medical centers said that the implemented functions of DHCP satisfactorily met their critical automated information needs and were beneficial in improving service to the veterans.

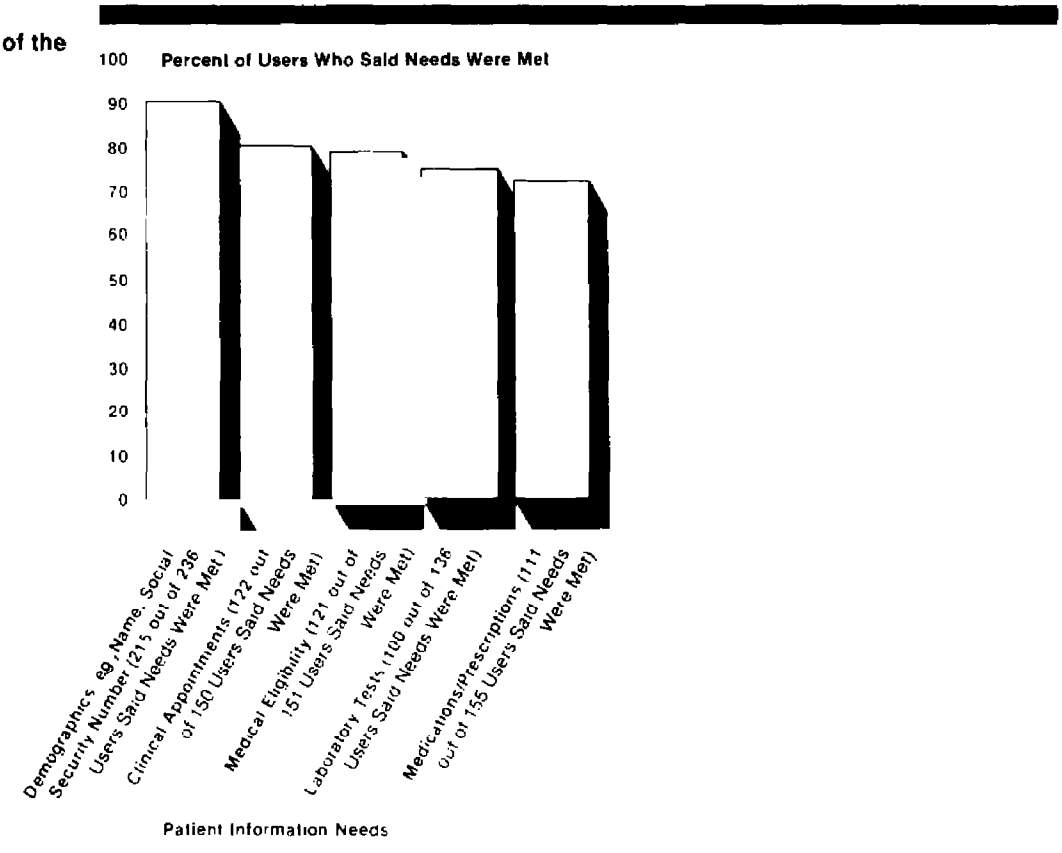
Basic Information Needs Met and System Users Satisfied at Sites Visited

Our interviews with 252 medical center users indicated that critical information they needed was available in the Core modules and that they were generally satisfied with DHCP system operations. According to these users, they wanted the system to have current patient and administrative data and be accessible to a wide variety of medical staff. Most users said their current DHCP system met these needs. Of the staff interviewed, "demographic information" was most frequently cited as the data "needed." Most of those who cited this need said their system provided this information. Among the other types of available data cited as needed were information on clinic appointments, medical eligibility, laboratory test results, and patient medications. Seventy-two to 81 percent of the users who said they need these data responded that their needs

[1]We used standard lists of questions to interview 13 medical center directors, 13 computer center site managers, 36 medical service chiefs, 34 application coordinators, and 252 system users.

were met. Figure 2.1 shows that the data cited by users as "needed" were generally met by the DHCP system.

Figure 2.1: DHCP Core Software Generally Met Informational Needs of the Users Interviewed

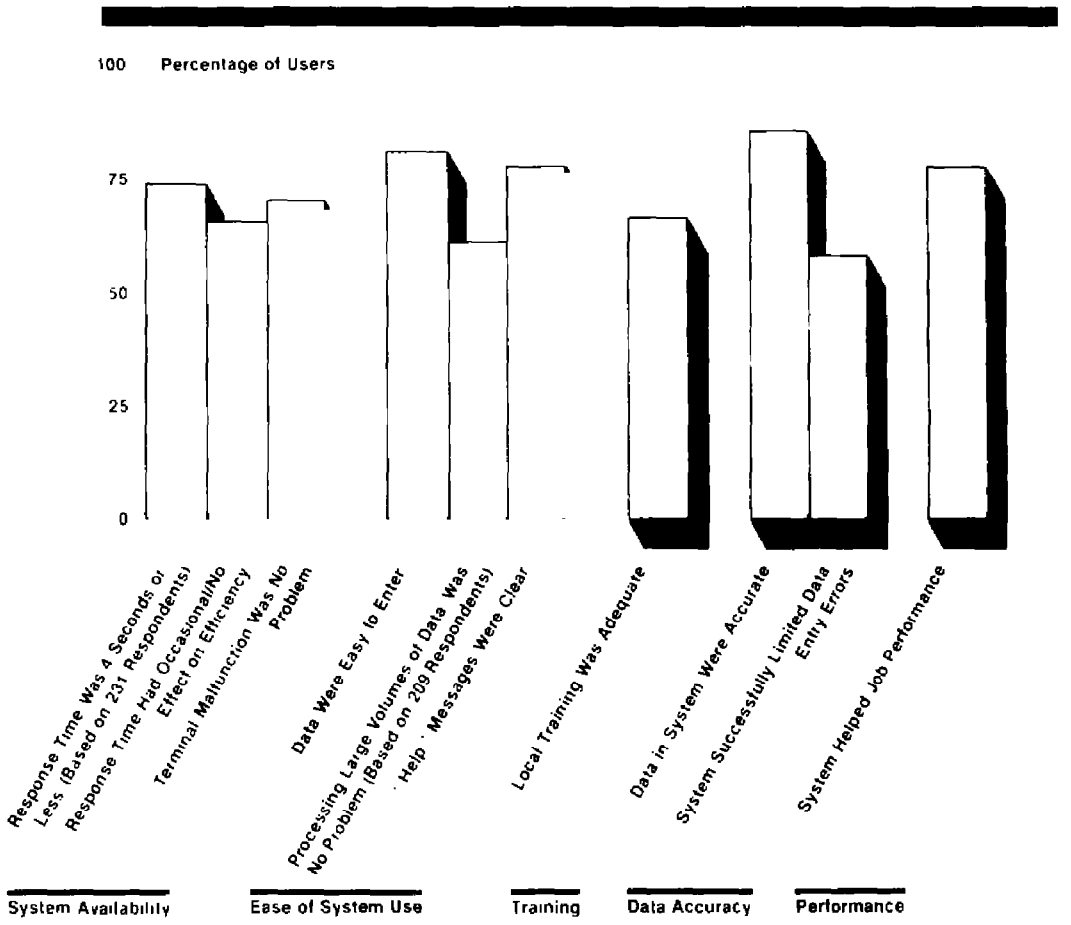


Note: These percentages represent the number of users who said that the system provided the information needed compared to the percentage of users who said that they needed the information to perform their job. We interviewed 252 users.

DHCP users were also generally satisfied with the computer system operations. As figure 2.2 shows, users told us that (1) the system generally responded in 4 seconds or less, (2) the system was relatively easy to use, (3) training for users was adequate, (4) data in the system were perceived as accurate, and (5) the system helped users perform their jobs.

The medical center directors said that the system had a positive effect on the centers' service to veterans. Most of the medical service chiefs and application coordinators commented that they believed the system was accurate. The site managers also had favorable comments; however,

Figure 2.2: Users Interviewed Were Satisfied With DHCP System



Note: Except as noted, percentages are based on the 252 users interviewed.

most said that their staff needed additional technical training on the computer equipment, programming, and the system software.

Decentralized System Has Benefits for Veterans and Users

The majority of the managers and users we interviewed concluded that DHCP was beneficial because it made patient data more readily accessible, which in turn improved the medical centers' service to the veterans. Several said, for example, that the system allowed staff on the hospital wards to access a patient's laboratory test results as soon as the technicians entered them into the data base. This reduced the number of phone calls for laboratory results and decreased the number of duplicate tests or lost results. Physicians told us that ready access to laboratory

results led to more timely diagnoses and better patient care. The pharmacy staff said that improved access to patients' current medication profiles allowed the veterans to receive their outpatient prescriptions quickly.

DHCP received a highly favorable rating over prior computer systems because it offered needed "flexibility." Of the 13 sites visited, 8 had some previous computer systems that had been replaced by DHCP modules. Officials said that, unlike DHCP, these previous systems offered little or no flexibility for system changes. The flexibility features of DHCP most often cited as needed were the abilities to locally tailor software and to operate additional software. According to officials, an example of local DHCP tailoring involves creating templates[2] to meet specific data needs of local medical centers.

Shortcomings of Initial Implementation Could Affect Patient Care

Although VA's decentralized management approach resulted in an expeditious implementation of DHCP that satisfied users' most critical needs, inadequate central control resulted in inconsistent and ineffective (1) software development, (2) software controls over patient records, and (3) internal controls over patient data and computer facilities. All of these conditions could affect patient care. VA is aware of these problems and has begun actions to correct them.

Inadequate Central Management Control: A Key Factor Contributing to System's Problems

Although decentralized management has been a contributing factor to VA's success in installing DHCP's Core modules and achieving user satisfaction, centralized management and authority are needed to appropriately address existing problems and efficiently correct them throughout the agency. Such central direction is consistent with the Administrator's February 18, 1982, Executive Order that was reaffirmed in his April 8, 1982, letter to the Chairman of the House Government Operations Committee. Specifically, VA's August 13, 1982, Circular 82-31 clarifying the Executive Order stated that the Chief Medical Director was authorized to establish the Medical Information Resources Management Office, "which will have overall responsibility for implementing the DHCP program and managing all departmental information management and ADP activities." The VA circular also stated that it was essential that lines of

[2]Templates are software tools used for saving specified fields of data that facilitate entry and retrieval in certain formats or to extract data for special purposes, such as a listing of veterans affected by Agent Orange herbicides.

authority and responsibility be clearly defined to ensure the success of the program

In establishing the Management Office, the Chief Medical Director followed the VA circular directive by making the office responsible for both ADP and information management, including authority over the Information Systems Centers. These centers were established to develop and verify software modules, provide technical expertise to the medical centers in their region, and support hardware and software implementation and maintenance of the decentralized system. In July 1983, however, VA changed its organizational structure to be most responsive to user needs and to focus on deploying equipment and implementing modules at the local medical centers. Under this reorganization, the supervision of the Information Systems Centers was changed from the Management Office to the Regional Directors who reported directly to the Department of Medicine and Surgery.

Thus, although the Management Office retained responsibility for ADP and information management, it no longer had authority to directly manage the software development and local computer procurement, installation, operation, and maintenance activities. For example, the office could not issue directives to the Information Systems Centers addressing such issues as required software development procedures without first receiving approval from the Regional Directors. Furthermore, under this organization, the Information Systems Centers were only to coordinate with the Management Office as they deemed appropriate.

In February 1987—as a result of discussions with us, cognizant congressional committees, and internal auditors, and after recognizing problems that were occurring under its decentralized management structure—VA changed its organizational structure and placed the Information Systems Centers personnel under the direct authority of the Management Office. VA commented that this change will strengthen national coordination and direction in order to meet such needs as system refinement, module interaction, software integrity, and standardization of day-to-day operations. VA also said that this realignment will serve to strengthen the project management and accountability on issues of national priority while retaining, in the regions and medical centers, the necessary degree of control required at those levels. We believe this change is a step in the right direction. Making one office accountable for ensuring that DHCP is effectively developed and implemented and providing the office with

the authority necessary to meet this accountability should help VA effectively implement and manage the DHCP system. This action should also help VA in avoiding the types of problems it encountered during the system's initial stages, as described in the following sections

Software Development Process Was Inconsistent and Ineffective

Federal guidelines call for agencies to ensure that their software is appropriately developed before releasing it for general use and to provide adequate documentation to facilitate operation, maintenance, and enhancements of the software. Software problems should also be consistently tracked agencywide so that corrections can be incorporated into future software releases and multiple sites will not waste resources trying to correct identical problems. We found, however, that VA was not adequately following these practices agencywide.

Office of Management and Budget circular A-130 requires agencies to (1) perform software tests before placing an application into operation and (2) develop information systems in a manner that will allow future expansion to be compatible with the existing system. Federal Information Processing Standards Publications 31, 38, 64, 102, and 105 state that

- new application software systems should be installed only after thorough program and system tests have been completed and approved;
- documentation should be performed during all phases of software development and operation; and
- programs should not be accepted without adequate and complete documentation (covering data, operations, system design, and program and acceptance tests) that an independent body has reviewed and approved.

Although DHCP's software development process included program testing at development centers and field testing at medical centers, during the initial years of software development for DHCP, VA did not have a software development policy addressing documentation, verification, testing, and approval procedures. In June 1985, over 2 years after VA began its decentralized software development, the Management Office released its first software development policy (Circular 10-85-93). However, this policy did not meet federal guidelines for software development because it did not address the critical procedures described above. Rather, it addressed such issues as how the files would be numbered, stated restrictions on adding new data elements, and strongly discouraged other types of local data modifications to the national software packages.

Management Office officials said that initially they chose to use informal rather than formal guidance because they did not have the technical staff to write policy and manage the overall system software development. Additionally, they said that, under VA's decentralized organization, (1) each of the Information Systems Centers is responsible for developing individual software modules for VA-wide use and for verifying modules developed by other centers, and (2) medical center administrators are responsible for their own computer centers and the effect of their computer systems on their medical centers.

However, in the absence of headquarters policy, the centers generally did not follow federal guidelines and developed and released software using a variety of informal testing, documentation, and verification procedures, which contributed to inadequate software development and premature software releases. For example, as discussed in the next section, some software was released without essential internal controls to prevent the (1) creation of multiple, incomplete patient records and (2) potential for unauthorized approval of patient services. Several site managers told us that they found problems with the initially released software. Numerous versions were frequently released following initial release, to correct deficiencies and make improvements. For example, in the worst situation we identified, one development center made 22 VA-wide releases of a software package between March 1984 and March 1985. A primary reason for these multiple releases was to correct problems that had not been identified during testing. Had adequate testing, documentation, and verification been performed, missing internal controls could have been included and other problems corrected before the software packages were released to VA's DHCP computer sites.

On December 9, 1986, the Management Office sent the Information Systems Center directors an "interim" detailed DHCP software verification policy statement to help prevent software problems and ensure that software releases would be technically correct. VA expects to issue a formal circular on this subject in October 1987. The software development problems we identified should be corrected if (1) the circular follows the interim policy statement in establishing appropriate testing, documentation, validation, and approval procedures, and (2) the Management Office ensures that the software developers comply with this policy.

In commenting on our draft report, VA stated that from 1983 to 1986 its number-one priority was to establish a baseline of Core software at the medical centers as quickly as possible to help facilities keep pace with the expanding work load. VA recognized, however, that this goal was

realized at the expense of thorough documentation and rigorous quality control. VA added that, in addition to the June 1985 software development policy circular and the December 9, 1986, interim software verification policy statement, it has taken other steps to improve compliance with federal guidelines. These include issuing software documentation guidelines on May 15, 1987, and adding additional positions for software verifiers and documenters.

VA also said that it is improving its documentation, verification, and testing procedures. For example, the agency said it has prohibited release of new modules without adequate user and technical documentation and estimates that the Core module documentation will be brought up-to-date by the end of 1987. VA said that documentation standards are being put in place and that responsibility for assuring conformance has been centralized in one location. The agency said that the quality of its software has been strengthened by having software packages verified by both the developing Information Systems Center and by another center prior to release for general use. Finally, VA said it has expanded its testing process to ensure that modules are tested at medical centers using VA's standard operating systems and the Federal Information Processing Standards programming language used in DHCP.

In addition to federal guidance on software development, it is also common practice in the software development industry to track software and hardware problems so that corrections and improvements can be incorporated in future software releases or made before acquiring additional hardware. Such tracking can prevent other sites that experience similar problems from expending unnecessary resources trying to correct them. VA emphasized rapid installation of the system and did not establish procedures for DHCP requiring that software and hardware problems be tracked and corrected.

We found that the Management Office did not identify and track software and hardware problems and that, left to their own initiative, only two of the six Information Systems Centers tracked such problems, resulting in ineffective problem correction. For example, the module handling data on admission, discharge, and transfer of patients provided incorrect statistical counts that were difficult to correct. However, absent VA-wide procedures on this issue, the responsible Information Systems Center made corrections for the individual medical centers that reported the problem instead of making one correction for VA-wide

implementation. VA is implementing an agencywide, error-tracking system for its laboratory module and will consider similar tracking reports for its other modules.

In responding to our draft report, VA said that tracking and correcting hardware and software problems is an ongoing process within the DHCP system and that it has multiple mechanisms for dealing with these problems. Examples VA provided included (1) the joint tracking of hardware problems by the site manager, vendor representatives, contracting officer, and responsible Information Systems Centers, and (2) the general reporting of application software problems reported through electronic mail, where problems are tracked by both the developing Information Systems Center (responsible for a solution) and the Management Office and where software corrections are available to all sites.

We found that although some Information Systems Centers tracked problems, the tracking was not done consistently VA-wide for efficient correction. VA concluded that although its procedures have proven effective, the procedures should be formalized, improved, and streamlined. VA said that work had begun on a DHCP project-tracking system for Management Office oversight and management of all department information resources. The agency added that, in April 1987, it had received the first quarterly status report from a recently implemented system to track the installation of both hardware and software. VA also stated that, as part of its improvements in this area, it has a contractor preparing specifications for a tracking system that will include, but not be limited to, program management issues and the tracking of national software development by the Information Systems Centers.

Software Controls Inadequate to Prevent Incorrect Entry of or Unauthorized Changes to Data

The Department of Medicine and Surgery's medical center procedures require that patient records be complete and accurate. However, we found that VA's software controls and medical center practices were not sufficient to prevent system users from inadvertently creating multiple and incomplete patient records or making unauthorized changes to veteran eligibility information. These insufficiencies have resulted in some inaccurate records in the DHCP system, which could result in VA's providing inadequate medical services or improper levels of service

Software Controls Do Not Adequately Prevent Accidental Creation of Multiple Patient Records

At the two medical centers where we performed tests to determine the adequacy of software controls to prevent or limit data entry errors and detect errors after entry, we found that over 100 multiple, incomplete patient records existed in the DHCP system. Staff at these medical centers expressed concern about the potential impact that multiple records could have on the quality of health care delivery. They also told us that even when they detected multiple patient records, they had no effective method for eliminating them. Because the other DHCP medical centers use the same software, we believe that the potential exists for similar problems at these centers.

The procedures for registering patients outlined in the DHCP user manuals instruct users to check first whether a patient's name is in the system before the patient is registered. Users are also instructed to enter last name, comma, first name, and then middle name or initial. Although the software prevents users from creating multiple records by entering an exact duplicate of a currently registered patient's name and social security number, it allows multiple records to be created through such deviations as capitalizing letters or allowing extra spaces between words.

We tested DHCP's software control effectiveness in preventing or detecting input errors by simulating patient registrations. With the system software, we were able to create multiple patient records by entering patient data that:

- Included blank spaces between words. For example, "DOE, JOHN" was established as a different patient from "DOE, JOHN."
- Inserted numeric digits within the name. For example, "D0E, JOHN," where the second character of "D0E" is a zero rather than the letter "O," was established as a multiple patient record.
- Used uppercase for the first initial of both the first and last names and then used uppercase for only the first initial of the last name. For example, "Doe, John," and "Doe, john" resulted in multiple records.

To determine the extent of multiple patient records at the two medical centers tested, we used a VA search program to locate and isolate potential multiple patient records. At the first site, we examined about 46,000 patient records and selected for review those records that appeared to belong to the same patient based on multiple common characteristics. The medical center staff identified 68 of the cases where, in fact, two records existed for the same patient. From a similar examination using about 34,000 patient records at the second site, the VA medical center

staff determined there were 73 multiple patient records. An official said that additional tests, using checks against more data elements, would probably yield a higher number of multiple patient records. We found that controls had not been incorporated in the software that would detect such input errors and there were no procedures for manual checks to detect these errors. The Management Office director said that the Office did not assign a high priority to including all key data controls in the software because of (1) the urgency of making the software available to medical centers and (2) VA's assumption that it would receive high-quality data input. He added that an updated version of this module, expected to be released in mid-1987, will include additional data input controls, which he believes will correct the problem.

A medical center director at one of the larger sites said entries in multiple records can result in incomplete patient records, and thus create the possibility of duplicating prescriptions or laboratory tests. A medical center official noted that multiple records could also result in doctors' making medical decisions without having a patient's complete record. Consequently, doctors may prescribe medications for a patient without the benefit of the patient's laboratory test results (for example, identification of a specific infection), and therefore may not prescribe appropriate medications. He also noted that rectifying multiple records can increase medical center costs. He estimated that his staff had identified 400 to 500 multiple patient records in their system.

Site managers at several medical centers stated that the system did not have an effective method for merging multiple records to correct patients' records. The software uses record pointers that establish linkages between patient data from the various modules that contain data on each patient in the data base. Therefore, when removing a multiple record from the system, medical center personnel must be sure to account for and combine all record pointers associated with the record. Otherwise, portions of the deleted record will not be added to the new record, and extraneous information will remain in the system.

Because system personnel had not developed a utility program that can identify all pointers associated with a particular record, the medical centers do not have a uniform method to reliably remove multiple records from the system. We found that staff from some medical centers were not removing multiple records after they were identified. Rather, they said that they mark the multiple patient records and plan to correct them when the software developers provide an effective method for merging such multiple records.

In commenting on our draft report, VA officials agreed that this area warranted their immediate attention. They stated that although they had corrected some of the conditions cited they found, "as the GAO report corroborated, that under some conditions it is still possible to create duplicate patient records." VA plans to use a two-pronged approach to minimize the problem. First, the agency plans to have staff identify and merge multiple patient records. Second, it is actively working on technical methods to ensure that data are accurately entered into the system. VA estimates that an automated, patient-record-merge routine will be available in late 1987. It also planned to release an interim software module in June 1987 that will automatically check several key indicators to identify possible duplicate entries before adding a new patient record.

Software Controls Did Not Adequately Prevent Alteration of Patient Eligibility Data

Veterans' eligibility for VA medical benefits is based on such factors as the type of illness sustained (service connected versus non-service connected), length of service, and type of discharge. When patients initially register at medical centers, they must present proof of eligibility. The registration clerk enters the appropriate eligibility code on the patient's record through a computer terminal. However, until the medical center receives verification of the patient's eligibility from a regional office, a patient's record shows eligibility as "not verified." After the regional office verifies a patient's eligibility and notifies the medical center, a medical administration clerk enters the verified eligibility code on the patient's record.

At several medical centers, we found that after a patient's record showed a verified eligibility code, this code could be changed by system users to make the patient eligible for more or fewer services. After these changes were made, however, the system did not label these changes as "not verified," but continued to show eligibility as "verified." An official told us that registration clerks, clinic clerks, and ward secretaries all had access to the eligibility code field. Thus, many computer system users could change patient eligibility codes, allowing patients greater medical benefits than they were entitled to receive.

In commenting on our draft report, VA cited several mechanisms, such as a security sign-on module, use of passwords, and limited user access, which it believes are "more than adequate to prevent unauthorized data entry." While these items are examples of controls over access to the

system, they do not prevent persons that are authorized to use the system from making unauthorized data entries and inappropriately changing a patient's eligibility status. VA commented that it had also identified this situation and corrected it in April 1987 when it released an updated version of the software package. According to VA:

"The software will now allow only a holder of a specific password to verify patient eligibility. Once eligibility has been verified, it is not possible to change the eligibility status unless one is also authorized to verify eligibility by virtue of possessing the password. In addition, when the eligibility status is updated after initial verification of eligibility, an audit trail is created identifying the authorized user responsible for the change."

Internal Controls Inadequate to Protect System and Patient Data

A principal objective of DHCP was to quickly provide all VA medical centers with comprehensive data processing systems for key functions. However, VA did not sufficiently address internal controls by establishing a policy that requires (1) performing risk analyses to assess security and controls over access to patient records, and (2) contingency planning for such events as natural disasters or emergencies. Although such controls are addressed in federal regulations and guidelines, headquarters officials said that they did not have enough staff to devote to developing policies. Management Office officials said that they believed that the software security programs, along with the site manager training offered prior to system installation, were sufficient.

It was not until August 1985, or 2 years following the first installation of DHCP hardware and software in medical centers, that the Department of Medicine and Surgery issued guidelines for establishing computer security procedures at VA medical centers. These guidelines, however, lacked key elements called for by federal regulations and guidelines and, under VA's decentralized management system, no reviews were made to ensure that the Information Systems Centers and medical centers complied with the guidelines that were issued. Consequently, the 13 medical centers we visited were not following federal guidelines on (1) implementing risk analysis and contingency planning, (2) controlling access to patient records, and (3) restricting release of software security information.

The lack of such controls, as well as the previously mentioned software development deficiencies, are material weaknesses under the Federal Managers' Financial Integrity Act 31 U.S.C. 3512(b) and (c). These

weaknesses are regarded as material, given the relative size and importance of DHCP to VA, the sensitivity of VA's patient records, and the necessity for maintaining complete and accurate records to ensure proper medical care of VA patients. In 1985 and 1986 the VA Administrator, in submitting his annual internal control reports to the President in accordance with the Financial Integrity Act, identified DHCP as a material weakness because of the concern over the adequacy of controls and of documentation concerning compliance with policy and regulations. VA recognizes the need for conducting risk analyses, developing contingency plans, and specifying levels of security. In commenting on our draft report, VA said it believed it had made substantial progress in this area and is continuing to strengthen this aspect of the program.

Risk Analyses and Contingency Plans Not Adequate to Protect Facilities and Equipment

Office of Management and Budget Circular A-130 requires agencies to provide appropriate internal controls over computer systems. This requirement includes conducting periodic risk analyses and developing appropriate contingency plans. Risk analyses are to be conducted at each computer site, both periodically and when a significant change occurs, such as adding telecommunications, to ensure that appropriate safeguards exist. A risk analysis evaluates security by considering the likelihood and cost of various security threats, such as system intrusion, that are present or that might occur during an average year. The absence of a risk analysis results in a lack of explicit criteria for selecting appropriate safeguards and for designing and evaluating contingency plans. We found that VA did not appropriately implement these requirements.

Contingency plans are to be developed in the event that computer support is interrupted by either an emergency or natural disaster, such as loss of electrical power or earthquake. The Office of Management and Budget Circular A-130 also requires that these plans be tested regularly. Contingency plans should include the steps to be taken immediately following an emergency to protect life and property, minimize the impact of the emergency, and address shutdown of the computer system to protect data. Without emergency procedures, the sites are vulnerable to unnecessary property damage, loss of computerized data, and human injury. Disaster recovery plans should include steps for the smooth, rapid restoration of the computer system, its data, and program files following physical destruction or damage. The lack of disaster recovery plans may result in difficulties and delays in restoring computer system operations following such damage or destruction. Failing to test such plans makes it difficult to determine if they are adequate.

At the 13 sites visited, we found that only 4 had performed a risk analysis. We also found that although 8 had developed contingency plans for emergency procedures (5 had adequately developed plans and 3 had partially developed plans), only 3 had tested their plans.

In December 1986, VA drafted an ADP circular that requires risk analyses and contingency plans at each ADP location. This draft circular specifies when risk analyses and contingency plans are to be conducted at Information Systems Centers and provides an audit guide for the Inspector General's use during review and oversight. The draft policy was transmitted to the centers on December 8, 1986, for interim use until an official circular could be issued.

In commenting on our draft report, VA agreed that it had not provided adequate guidance to the computer sites; consequently, the thoroughness of risk analysis and contingency planning varied from site to site. VA said its ADP security policy circular is being revised and would be reissued in October 1987; it will have, in addition to an ADP security policy that applies to all department offices and facilities, guidelines for the medical centers, Information Systems Centers, and VA central office. VA said the new circular will serve as the basis for each entity to develop specific procedures for its individual requirements. VA also said that (1) in February 1987 additional positions were approved to add staff to monitor compliance with department policy and guidelines and (2) effective October 1986, it had obtained a vendor contingency maintenance program to replace appropriate DHCP system components within 2 to 14 days following a disaster at all but its smallest medical facilities. VA also stated that it was currently negotiating for coverage of the smallest sites.

Access to Patient Records Not Adequately Controlled Through Security Clearances

Office of Management and Budget Circular A-130 requires agencies to establish security commensurate with the sensitivity of the information and ensure that only authorized personnel have access to the information system. Office of Personnel Management's Federal Personnel Manual chapters 732-2 and 736 state that agencies are to have procedures to ensure that security clearances are issued for (1) "Critical Sensitive Level" positions involving major responsibility for systems hardware and software, and (2) "Non-Critical Sensitive Level" positions involving personnel that direct, plan, design, operate, or maintain a computer system. Appropriate background checks are supposed to be conducted before clearances are issued. While VA's August 1985 policy addressed

ADP security at all medical centers and defined levels of security clearance, it did not require that key system personnel receive a specific level of clearance supported by an appropriate background check. We found that many key personnel with access to sensitive data, such as site managers, programmers, and other personnel responsible for designing and operating the system, did not have appropriate security clearances.

At the time of our review, 164 computer center site managers had access to sensitive patient data. On the basis of information obtained from VA's Office of the Inspector General and medical center personnel offices, we found that 116 of the site managers (or 71 percent) had no record documenting an appropriate security clearance. From a second list of 147 Information Systems Center employees we randomly selected 35 names and found that

- 25 had no record documenting an appropriate security clearance,
- 9 had been assigned an appropriate security clearance, and
- 1 was no longer a VA employee.

By not justifying the level of access and determining the security fitness of its personnel, VA is exposing sensitive patient data to the risk of theft, deliberate disclosure, or alteration. The draft December 1986 security policy circular specifies the level of security clearance required by Information Systems Centers' personnel, but does not address the security clearance levels required by the medical center personnel. The Management Office director said he plans to use the December 1986 draft circular as a guide to update the August 1985 policy that addresses the medical centers' role. He said the Management Office would transmit this interim policy soon, for use by the centers until the official circular is issued. VA estimates this circular will be released in October 1987.

Releasing Software Under the Freedom of Information Act Increases Risk of Unauthorized Access

On the basis of a January 27, 1982, decision by the VA Administrator, VA routinely releases DHCP software, such as the laboratory modules and related documentation, to outside organizations and individuals upon request under the Freedom of Information Act. The previously mentioned internal control weaknesses in the system, combined with the unrestricted release of the software, increase the risk of wrongful access to and disclosure of VA's patient medical records and other sensitive data.

In January 1982, the VA Administrator responded to an appeal under the Freedom of Information Act for the release of software and documentation of another computer project—the Medical Administration Health Care Information System. The act requires agencies to disclose records upon request by the public, unless the records are otherwise exempted from disclosure (5 U.S.C. 552(a) and (b)). The Administrator concluded that VA was required under the act to release the requested computer programs and documentation, except for the individually identifiable patient data bank, security codes, and security programs. This information was withheld under several of the act's exemptions.[1] The Administrator's decision indicated that withholding the individually identifiable patient data bank was appropriate because the data bank contained personal medical information concerning VA hospital patients. The decision noted that withholding the security codes and security programs was proper because their release would directly compromise the security of the data bank and expose the confidential information contained in it to unauthorized disclosure.

VA officials told us that they frequently release DHCP's software and documentation to the public upon request. They explained, however, that they restrict release of the patient data bank, security codes, and security programs on the basis of the January 1982 Administrator's decision. We found that although VA restricted release of such information to requesters, it released other critical information, namely DHCP's security parameters, that could facilitate unauthorized access to the patient data base. This information describes VA's software security and states the number of characters and other information that could be used to access the system. Since the release of this information may compromise the security of the patient data base, we believe it is not consistent with the Administrator's decision that states that the patient data base should be protected. During our review we brought this issue to the attention of both the VA Inspector General and VA program officials. VA officials shared our view and, following discussions with us and their Inspector General, in June 1986, VA officials requested that their General Counsel restudy this issue.

In responding to our draft report, VA stated that its General Counsel's response indicated that the Freedom of Information Act exemptions permit discretionary withholding of software that controls access to DHCP or

[1]These exemptions pertain to matters that are (1) related solely to an agency's internal personnel rules and practices, (2) specifically exempted from disclosure by statute (that is, 38 U.S.C. 3301(a) and 4132(a)), and (3) personnel and medical files and similar files that by disclosure would constitute a clearly unwarranted invasion of personal privacy.

that ensures the integrity of applications processing and internal controls. Consequently, VA said it is finalizing a circular that will implement this discretionary authority and has implemented the practice of discretionary disclosure prior to releasing the circular. VA also said it now has two versions of the software application that controls access to DHCP—one that contains sensitive data and is distributed only within VA, and one "public domain" version with these data deleted.

DHCP Expansion Planned Without Information Necessary for Informed Decisions

VA is preparing to expand DHCP at an estimated cost of $385 million for additional hardware, software development resources, and personnel support through fiscal year 1996 for eight Enhanced modules. VA's estimated total life-cycle cost of the Core modules plus the eight Enhanced modules is $925 million. This expanded, more complex system is intended to automate additional functions needed to further support the requirements of medical center users. The expansion also includes meeting objectives important to the system's success, such as effectively obtaining the data needed by all hospital services and linking the medical centers, regional offices, and headquarters.

While VA has done some analysis to justify its planned expansion, it has not adequately analyzed alternatives to ensure that the most cost-effective approach has been selected. In a period when there are many important competing demands on the federal budget, federal agencies and the Congress need assurance to make informed decisions on expansion. VA is also making decisions on the need for computers and their allocation to sites without considering current computer use and capacity. Also, until May 1987, VA had not given adequate management attention to the development of a key software feature that is an important objective of DHCP.

Expansion Plans Include Substantial Amounts of Software, Hardware, and Telecommunications

VA plans to supplement its six Core modules by implementing eight Enhanced modules in its system during fiscal years 1987 through 1996. These Enhanced modules will provide needed automation to such areas as radiology, surgery, and nursing. One of the top-priority Enhanced modules, the decentralized medical management system will provide VA-wide medical, financial, and administrative data for decision-making purposes. In this module, certain data will be extracted from the data base in each local medical center for use by local management and aggregated for use at the regional and headquarters level for budget and resource allocation decisions. VA plans to have this module link costs with patient care provided, thus allowing better cost assessment by type of patient diagnosis. As part of the Enhanced module development, an order entry/results reporting feature is also planned that will allow users to quickly access data. VA officials believe this feature is important to the program. VA estimates the majority of computer hardware to support the eight Enhanced modules will cost about $84 million and plans to incrementally procure this equipment during fiscal years 1988 through 1990.

In February 1987, VA's planned DHCP system consisted of 6 Core, 22 Enhanced, and 23 Comprehensive modules covering a 19-year life cycle. In June 5, 1987, comments on our draft report, VA stated that it had limited DHCP to a 10-year life cycle with 6 Core modules plus 8 Enhanced modules whose costs have been justified and approved. VA indicated that the remaining 14 Enhanced modules and the 23 Comprehensive modules are now only potential areas for future automation.

VA also plans to replace its current agencywide telecommunications system with a new telecommunications network during fiscal years 1987 and 1988 and operate it for 10 years. VA's plans show that a major portion of this network will be used to support the DHCP system to facilitate the exchange of data between the Departments of Medicine and Surgery and Veterans Benefits.

Latest Cost/Benefit Analysis Did Not Include Consideration of Hardware Configuration Alternatives

In planning for its DHCP expansion, VA did not adequately consider feasible configuration alternatives that could reduce costs. Also, VA had not prepared an adequate cost/benefit analysis before proceeding with its procurement process. The limited analysis that was prepared in 1986 for the fiscal year 1988 DHCP budget request did not include some significant costs; nor did the analysis appropriately develop and document estimated cost savings and benefits.

In commenting on our draft report, VA stated that many of the points we had raised regarding the 1986 cost/benefit analysis of the Enhanced DHCP system were valid. To respond to these points, VA had a consultant update and revise its cost/benefit analysis to provide better support for expanding the Core DHCP system with eight Enhanced modules. Although we did not assess this revised analysis in detail, we noted that VA had included more complete cost categories and additional nonquantifiable benefits. However, the revised analysis considered only one alternative—comparing the present manual system with the eight modules supported by a decentralized hardware configuration with on-site computers. Although the revised analysis is more complete, without considering feasible alternatives, VA has not taken the steps necessary to ensure that the most cost-effective hardware configuration will be selected.

DHCP System and Life-Cycle Cost Estimates Have Increased and Include More Complete Cost Categories

In 1983, VA's originally planned DHCP system included a total of 11 modules at an estimated 7-year, life-cycle cost of $155 million in 1983 dollars. VA's currently planned system includes 14 modules at an estimated 10-year, life-cycle cost of $925 million in 1987 dollars.

Federal Information Resources Management Regulations 201-16 and 201-20 and Office of Management and Budget Circular A-109 direct agencies to project life-cycle costs before acquiring major systems. These requirements were developed to help management obtain a reasonable understanding of the total cost of planned systems and assist them in making acquisition decisions. This circular defines life-cycle costs as the sum total of the direct, indirect, recurring, nonrecurring, and other related costs incurred, or estimated to be incurred, in the design, development, production, operation, maintenance, and support of a major system over its anticipated useful life span. Also, Office of Management and Budget Circulars A-121, A-130, and A-11 and Federal Information Processing Standards Publication 64 cite costs that agencies should consider. These costs include personnel; hardware equipment; software; supplies; utilities; site preparation expenses; and contracted services, such as telecommunications. According to these federal guidelines, agencies should account for the full cost of major information technology initiatives. (See appendix IV for a complete listing of cost elements and applicable federal guidelines.)

During DHCP development, VA identified additional data needs and added numerous software modules to its system plans. These additions substantially increased the cost estimates for computer equipment and personnel needs. In 1983, VA estimated that the total planned DHCP system would cost $155 million in 1983 dollars. However, by February 1986, VA had redefined its system several times, included the cost of 51 fully supported modules, added additional cost categories, and decided to use three overlapping, 10-year life cycles through 2001. These changes raised the estimated total DHCP cost to $1.2 billion in 1986 dollars (approximately $1.1 billion in 1983 dollars).

Prior to February 1986, the DHCP life-cycle cost estimates prepared by the Management Office were based on incomplete information because appropriate data were not obtained. For example, VA officials estimated the cost of DHCP personnel and computer equipment without determining the total number of staff assigned to support the system or obtaining an inventory of the computer equipment and operating software in the medical centers. Because of congressional interest and questions we raised during our review, VA significantly improved the accuracy of its

life-cycle cost estimate in 1986 by (1) obtaining and using information from the computer sites to develop cost estimates, and (2) better addressing life-cycle cost elements cited in federal guidance. However, the 1986 estimate also omitted and understated certain costs

Through analysis of VA's 1986 DHCP life-cycle cost estimate and discussions with VA officials, we identified three major areas of costs that were either omitted or understated. These included omitted recurring costs such as supplies, understated costs for site preparation and site staffing, and omitted costs for such categories as telecommunications, utilities, and computer-support personnel. We did not fully calculate all the omitted and underestimated costs and, in some instances, we relied on the judgmental estimates of VA officials. Nonetheless, we believed that these omissions—which could total $700 million—were substantial.

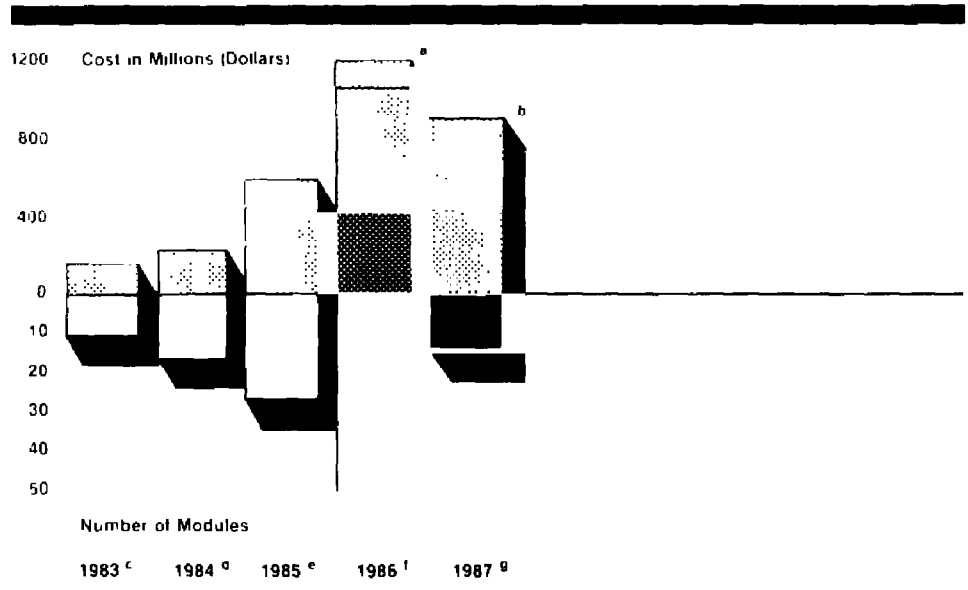
In a June 5, 1987, response to our draft report, VA stated that the scope of DHCP had been reduced to 14 modules at an estimated 10-year, life-cycle cost of $925 million in 1987 dollars. VA added that the omitted cost categories we had identified were included in its latest estimate. Figure 3.1 illustrates the change in software and life-cycle cost estimates.

Latest Decentralized System Cost/Benefit Analysis More Complete

In September 1986, in response to Office of Management and Budget Circular A-11, VA submitted a cost/benefit analysis to the Office of Management and Budget with its fiscal year 1988 DHCP budget request. In this submission, VA requested funds to procure hardware to fully support the Core modules and nine Enhanced modules. The analysis stated that the 1987-1988 requested computer equipment investment would result in 9.8-percent annual rate of return to the government and estimated the net savings in personnel and supplies over the Enhanced modules' 10-year life cycle at $46 million. The analysis also provided qualitative benefits for the nine modules. In our draft report we described VA's 1986 analysis and concluded that it lacked sufficient detail supporting the projected costs and benefits of the system.

In response to the deficiencies noted in our draft report, VA had a consultant revise and update its cost/benefit analysis. The new analysis shows a 9-percent rate of return to the government and a net savings with a present value of negative $5.5 million, using a 10-percent discount rate. VA stated that this analysis is conservative in that no attempt was made

Figure 3.1: VA's Decentralized System and Life-Cycle Cost Estimates (By Fiscal Year)



[a]Includes 6 Core Modules at $415 Million, 22 Enhanced Modules at $620 Million, and 23 Comprehensive Modules at $140 Million

[b]Includes 6 Core Modules at $540 Million and 8 Enhanced Modules at $385 Million

[c]$155 Million in 1983 Dollars

[d]$204 Million in 1984 Dollars

[e]$580 Million in 1985 Dollars

[f]$1 175 Billion in 1986 Dollars

[g]$925 Million in 1987 Dollars

Note: Cost data developed by VA. Numbers are rounded

to place a dollar value on qualitative benefits.[1] VA stated that this analysis

- covers eight rather than the previously planned nine Enhanced modules and does not include the six Core modules,
- uses a new implementation schedule reflecting the current budget and procurement schedule,
- uses revised life-cycle cost estimates that have been corrected to rectify omissions identified by GAO and updated to reflect policy changes,
- revises benefits to take account of changes in fringe benefits and in functionality,

[1]The two VA consultants involved with the two cost analyses (the complete 14-module DHCP system and the 8-module Enhancement part of the system) qualified their work by stating that they used data provided by VA and reviewed the data for reasonableness.

- uses revised estimates for anticipated salary increases, and
- follows the Federal Information Processing Standards Publication 64 insofar as that is feasible and appropriate.

We did not assess the revised analysis in detail. However, we verified that it did include the omitted cost categories identified in our draft report and more clearly identified the benefits to be realized. Furthermore, we agree with VA that its cost/benefit analyses demonstrate that it is worthwhile to computerize VA hospitals. However, as discussed below, VA is not taking advantage of available (prototype) cost and benefit data to assure itself that the most reliable estimates, given available data, are presented.

VA's prototype software development process provides a unique opportunity for assessing actual site-specific cost/benefit data that can be used to help officials estimate planned system costs and benefits. Through prototyping, VA develops modules at one Information Systems Center and tests them at several medical centers before implementing them throughout VA. If data on costs and benefits were collected at the test sites, VA officials would have actual operational data to assist them in determining if their planned modules were cost-effective. The Management Office director said VA plans to assess the total costs and benefits following VA-wide implementation of these modules.

In commenting on our draft report, VA stated that it believed a cost/benefit analysis based on a clear understanding of the planned system—and using program experts to estimate the impact on operations—was "preferable" to a methodology requiring new site-specific data collection. VA said it would continue to refine the cost estimates and monitor the benefits as software is more fully developed and tested, and would continue to conduct post-implementation evaluations on all applications. We agree that a post-implementation cost/benefit assessment can be useful in assessing the value of a system. However, the most accurate information possible should be collected and analyzed to help program experts make better estimates and more informed decisions regarding the related requirements and costs and benefits of major expansion plans. Cost and benefit data collected at the prototype sites would assist VA in making cost/benefit analyses and in refining mathematical models used to project equipment.

Alternative Hardware Configurations Not Adequately Assessed

VA cannot be assured that the most cost-effective system configuration will be used to meet its needs because it has not adequately assessed alternatives such as regionalization. A regionalized approach would use one computer to support distributed processing in several medical centers, as compared to VA's planned decentralized approach of placing a computer in each medical center. The Federal Information Resources Management Regulation requires agencies to (1) perform a comparative cost analysis of various ADP alternatives when replacing an installed ADP system to increase data processing capacity (section 201-30.009) and (2) consider the operational and economic feasibility of alternatives for the acquisition of ADP capabilities (section 201-20.003). This work is required to determine which alternative will best meet the users' needs "at the lowest overall cost over the system/item life."

Federal Information Processing Standards Publication 64 states that when preparing a cost/benefit analysis, alternative systems should be evaluated and compared with the existing system to determine the most cost-effective approach to meeting agency objectives. To do this, the publication states that the technical and operational characteristics of the proposed system and alternatives should be considered, such as various hardware configurations. Although VA plans to competitively procure hardware for its expanded system, it has selected a decentralized hardware configuration with on-site computers without considering the cost-effectiveness of other alternatives, such as regionalized computer centers or a combination of these approaches.

VA officials cited two reasons for considering only one configuration. First, Management Office officials said that a decentralized hardware configuration approach for automating medical centers met VA's needs because a main objective of DHCP was to allow the local medical center managers to control their individual computers. Second, VA officials told us they had not considered other hardware configurations for the next planned procurement for DHCP because the Congress directed them to use the decentralized system.

The 1983 Appropriations Conference Committee directed VA to continue with all deliberate speed and without further delay in the installation of DHCP in order to provide systemwide data to the agency. The Conference Committee also directed VA to discontinue development of a regional computer configuration (the Computerized Medical Information Support System) that was being managed by a different VA department than the one managing DHCP. This direction stemmed from the House Appropriations Committee, which had directed VA to cease development of the

regional system because it was "conceptually and technically redundant" with the current DHCP effort. The Committee also stated that this regional system was a "duplicative cost, [and] a major waste of expert staff resources." The Conference Committee was not restricting VA from considering various computer hardware configurations for DHCP but rather was directing VA to discontinue duplicative hospital system development that had been ongoing for about a year.

Two hardware vendors told us that, under current computer technology, a central computer center can provide service to multiple facilities through high-speed telecommunications that is similar to the service offered with a computer in every facility. Several hardware and software vendors indicated that either on-site computers, regionalized hardware, or a combination of both approaches can be cost-effective, depending upon circumstances, such as the amount of work load, number of users, telecommunications requirements, location of facilities, and operations and maintenance requirements.

In its June 5, 1987, comments on our draft report, VA stated that:

- VA reviewed the sections of the Federal Information Resources Management Regulation we cited and, after meeting with General Services Administration officials, determined that VA was in full compliance with these sections.
- VA rejected a regionalized systems approach because this approach compromised critical aspects of the agency's information management program. According to VA, "Computers are a critical resource of hospital managers and they should be able to control and be responsible for them as for any other resource in a hospital." VA concluded that "Use of regional computers for local operations is not acceptable to the VA."
- The regionalized Computerized Medical Information Support System was terminated after congressional review, and VA does not intend to restudy the issue of regionalization of local processing.
- Regionalization was "implicitly evaluated and determined not to be cost-effective for providing computer support to VA medical centers." VA added that regionalized systems are also inefficient and nonresponsive to users.

Although VA provided several reasons for not considering regionalization as part of its DHCP hardware configuration, in our view VA has not done sufficient in-depth analysis of alternative configurations to adequately demonstrate that its decentralized approach is a cost-effective approach to meeting its needs. First, although the Federal Information Resources

Management Regulation (section 201-30.009) does not specifically state that a regionalized approach has to be considered as an alternative approach, it states that consideration of alternatives is required to determine which approach will meet users' needs "at the lowest overall cost over the systems item life." The Federal Information Processing Standards Publication 64 provides additional cost/benefit analysis guidance on this issue and specifically states that "alternative approaches" should be evaluated to determine the most cost-effective approach to meeting agency objectives. However, VA said it did not consider a regionalized configuration because its purpose was to determine whether to extend the existing decentralized system. Second, hardware vendors have stated that, under current technology, regionalized systems can be designed to offer service similar to decentralized systems and that regionalized systems may be less costly. Thus, regionalization may offer VA hospital managers the computerization control they need at a lower cost. Third, although the earlier VA regionalized system was terminated after congressional review, the Conference Committee statements indicate that this system was terminated because it was redundant with DHCP, not because it was a regionalized system. Finally, evaluation of the cost effectiveness of regionalized computers, on-site computers, or a combination of both approaches for DHCP is a complex issue. Consequently, the cost effectiveness of regionalization cannot be adequately assessed from an "implicit" evaluation.

Although VA listed several possible disadvantages of regionalization, it did not perform an analysis to support its conclusion regarding the use of a regionalized approach within its decentralized system or assess the potential cost savings in such areas as hardware, site preparation, and personnel support. Furthermore, VA is currently using limited telecommunications and a partially regionalized approach to serve some of its outpatient clinics and at least one hospital from remote computer sites. The following VA comments and our responses suggest the weaknesses of such an "implicit" evaluation.

VA Comment

"Due to the highly interactive multitransactional use of DHCP applications, such as MAS [Medical Administration Service] and laboratory, required for effective operational support of VAMC [VA Medical Center] functions, any regionalization or centralization scenario will cause national telecommunications costs to soar."

GAO Response

Although telecommunications costs would increase under a regional approach, such increases potentially would be offset by decreases in

other costs. For example, using several regional computer centers serving multiple facilities rather than on-site computers at each medical facility should result in reduced hardware costs, preparation of fewer computer sites, and fewer personnel required to operate and maintain the total system. An assessment of regionalization as well as a combination of regionalized and decentralized approaches would indicate whether cost savings under such alternatives would outweigh any increase in telecommunications costs. Furthermore, VA apparently did not completely rule out the possibility of a regional approach when discussing the possibility of using commercial vendors because it stated: "Moreover, in the unlikely event that local performance and response requirements could be met without driving telecommunications costs to unacceptable levels, such regionalization could be achieved in-house through DHCP." As we have stated, a detailed analysis would be required to adequately assess the net effect of system configuration alternatives.

VA Comment

"Regional or central computer installations that serve multiple VAMC's are necessarily more complex than single hospital systems and pose significantly increased management and technical problems."

GAO Response

Even though some increased management and technical problems might occur, these problems could be addressed by placing highly qualified managers and technicians at the regional computer centers. Conversely, under a decentralized approach these scarce resources would have to be distributed among VA's 172 medical centers. Furthermore, the extent of the technical problems may not be more complex, as indicated by the fact that the same DHCP software modules would be used in both regional and decentralized systems, and VA currently links 55 of its outpatient clinics and at least one hospital to remote computer sites at its larger medical centers.

VA Comment

"Consequences of systems failure are greater because several VAMC's would lose their processing capabilities at the same time."

GAO Response

If a regional system failed it could affect several medical centers. However, a regional system provides opportunities to (1) offer more complete back-up service, (2) provide more highly skilled personnel on a round-the-clock basis (VA currently does not provide 24-hour coverage at

all of its decentralized facilities), and (3) offer more frequent and extensive maintenance (which is difficult to achieve at 172 sites with scarce resources), thus reducing the probability of system failure.

VA Comment

"On-site help is not available to solve hardware or software problems if a user at one of the VAMC's (e.g., a physician, pharmacist, or nurse) encounters a problem."

GAO Response

Even in a regionalized approach, individual sites should have a minimum of staff available, such as applications coordinators, to assist the users. Furthermore, as stated above, more qualified assistance than that offered under a decentralized approach would be available at the regional centers. In addition, VA could continue to support local sites with its regional Information Service Centers. VA stated in its comments that these centers are responsible for tracking and helping resolve hardware and software problems at computer sites under their jurisdiction.

VA Comment

"Remote systems become increasingly bureaucratic and unresponsive to users. This was a problem in the past and was one of the major reasons for implementing a decentralized system to support local hospital operations."

GAO Response

Remote systems do require a certain amount of consistency among users. For example, standard terms, shared data bases, and standard programs are used; however, the integrated DHCP system already has these characteristics. Furthermore, these characteristics are required to successfully implement VA's top-priority Decentralized Medical Management System, which includes reporting data to local, regional, and headquarters management. Also, in some instances regional systems offer better service to local hospital operations. For example, hardware and software repairs and upgrades can be made more quickly and with better quality control at a limited number of regional centers than at 172 decentralized sites.

System Utilization and Capacity Statistics Not Being Obtained for Planned Procurement

VA has not been consistently monitoring the use and available capacity of its DHCP computers to obtain data necessary for meeting local needs and effectively planning for future expansion. We found at the medical centers visited that these sites were not required to regularly monitor or report their computer usage and available capacity to the Management Office. The Management Office had not issued policy to require such

monitoring because under its decentralized approach it allowed the hospital directors to manage their own facilities. Although VA recently recognized that such data would help officials make better decisions, it does not have the computer utilization statistics required to efficiently plan for the computer replacement and major expansion.

The Management Office director said that the amount of computer hardware to support Full Core modules was understated and that capacity will be exhausted when the inpatient pharmacy is added, or sooner, if several of the other software modules are used on the system. To adequately support the Core modules and the planned Enhanced modules at the medical centers, VA plans to incrementally procure additional hardware during fiscal years 1987 through 1996 at a total estimated cost of $145 million.

Federal Information Resources Management Regulation 201-30.007 requires agencies to base the acquisition of new or additional computer resources on a determination of need supported by a requirements analysis commensurate with the size and complexity of the need. VA's plans for procuring additional computer hardware for DHCP are based on a recent sizing model that shows VA hardware requirements at the medical centers. This model was developed from actual and estimated work-load data and input by user groups, software developers, and medical center directors. VA plans to add greater-capacity computers to its large sites and move the existing computers from these sites to its medium and small sites. However, VA officials are making these decisions without complete information on existing computer systems' utilization and available capacity under current processing work loads. Consequently, neither the site managers nor VA headquarters has the information needed to determine whether the system's equipment requirements for individual medical centers are understated or overstated or whether the computers being installed will be adequate.

In December 1986, VA officials asked the Federal Computer Performance Evaluation and Simulation Center to evaluate the areas of performance management, configuration management, and capacity planning and how they might be improved. VA plans to use the results of this study to improve its capacity management. However, the Center's study and VA procurement decisions will be limited by the lack of ADP data on each site's available capacity and computer performance.

In commenting on this issue in our draft report, VA disagreed with our observation that it was not regularly monitoring the use and available

capacity of its computers. VA stated regular monitoring of computer utilization and available capacity is an integral part of good site management, that site managers had access to applicable vendor-supplied software routines and tuning guidelines from their Information Systems Center to assist in obtaining maximum efficiency from systems, and that other performance tools and documentation were being developed. Although VA stated that monitoring assistance was available for local site managers' use, it did not dispute our statement that the sites were not "required" to regularly monitor and report their computer usage and available capacity to the Management Office. As we discussed earlier, in our visits to sites, we found that computer utilization and capacity was not being regularly monitored. Also, VA did not dispute our statements that VA management does not have VA-wide computer utilization statistics required to effectively plan for computer replacements and major expansion.

Central Management Not Ensuring Consensus on Key Data in Order Entry/Results Reporting Feature

A primary objective of DHCP is to enable users at each medical center to efficiently obtain integrated patient data from all hospital service areas. Under its expanded system, VA plans to develop an order entry/results reporting feature that will allow users to quickly access patient data currently located in several different modules. However, we found that this feature's development was being delayed because consensus could not be reached on the necessary data requirements. This occurred because the Management Office did not assume the leadership role required to ensure that the various organizations involved reached agreement on this issue.

Although the current system's data base is integrated, it is less efficient than it could be because it has a limited order entry/results reporting capability. This limitation requires extra time to order items or obtain results from two or more modules. For example, from a nurses' station terminal, laboratory tests and medications can be ordered for the same patient in two ways. The laboratory and pharmacy modules can be individually accessed to order these items, or a special order entry menu can be developed to access these two modules upon request. However, both methods require multiple keystrokes and considerable time. On the other hand, the order entry/results reporting feature would allow more efficient access to data originating from service areas such as the pharmacy, laboratory, or nursing stations.

A special-interest group consisting of software developers and medical center user representatives was formed in 1985 to identify the common

information needs of each service and the interrelationships among those needs. However, officials said the medical center services could not agree on the data elements needed. The Management Office relied on the software developers to coordinate this effort; however, the special-interest group had met infrequently and had not resolved its differences. In 1986 the Management Office recognized the need for additional central management involvement and brought the special-interest group under its direction. However, this Office had not taken the leadership role required to ensure that the feature was efficiently developed. A Management Office official said that because of travel fund limitations, group members exchanged comments through their electronic mail system rather than meeting formally. An official told us that the responsible parties are working to resolve differences but added that a completion date has not been determined.

In commenting on our draft report, VA stated that it has accelerated development of the order entry/results reporting feature to the number-one priority for the Information Systems Centers. VA added that, in May 1987, developers and users met to resolve outstanding issues and agreed to necessary software changes. VA said the most important feature of this utility will allow users to access patient data originating in various modules with a single keystroke and display them on a single screen. It said the first version (containing three of five planned capabilities) will be available for final testing this summer.

Commercial Systems' Test Not Appropriately Structured to Compare Costs and Benefits

In 1980 the Appropriations Conference Committee directed VA to determine whether commercial computer systems or VA's system would be the "most cost-effective and of maximum value" to its vast medical center work. Before installing systems agencywide, VA was to analyze various alternatives using suitable test and validation methods that would pursue appropriate functional and integrated capabilities. In 1983, the Appropriations Committees directed[1] VA to conduct tests of commercially available medical information systems at three medical centers of varying sizes and appropriated funds in the fiscal year 1984 Appropriations Act to begin these tests. In August 1984 VA awarded separate contracts to three vendors totaling, according to VA, approximately $22.6 million These vendors began installing their commercial systems in September 1984 for a 36-month demonstration test.

We found that the basic features offered by the three commercial systems were similar to those offered by DHCP and, like the DHCP users, the commercial systems' users generally were satisfied with the services being provided. However, the demonstration test as conducted will not provide VA with the information necessary to directly compare the commercial systems to DHCP. Because of provisions in the vendors' contracts, the commercial systems being tested offer fewer features overall, and cost more than DHCP's estimated life-cycle cost. In commenting on a draft of this report, VA stated that we had correctly pointed out that DHCP and the demonstration test were originally conceived with different purposes and scope. VA said the test was not intended as a vehicle for comparing commercial systems with DHCP.

Commercial Systems and DHCP Have Similar Basic Computer Functions and Levels of User Satisfaction

We found that users of the three commercial systems, like DHCP users, were satisfied with their systems. VA awarded contracts for the demonstration tests of three commercial systems to: Shared Medical Systems at the Philadelphia, Pa., medical center; McDonnell Douglas Health Care Systems at the Saginaw, Mich., medical center; and Electronic Data Systems at the Big Spring, Tex., medical center. VA service chiefs and system users at the three sites told us that the computerized information needed to perform their jobs generally was provided by their respective commercial systems. The required information most frequently cited was for patient demographics, laboratory tests, and medications/prescriptions. Table 4.1 shows the percentage of 58 users who responded positively

[1] During fiscal years 1983-1987, the Congress also appropriated funds to develop, implement, and operate DHCP

when asked whether their system provided the types of information needed to perform their jobs.

Table 4.1: Commercial-System Test Sites Generally Met Information Needs of Users Interviewed

(Percent of users' needs met)[a]

Patient Information Needed By System Users	Commercial Test Sites		
	Philadelphia	Saginaw	Big Spring
Demographics	81	94	72
Laboratory tests	80	92	81
Medications/ Prescriptions	[b]	73	71

[a]Based on interviews with a total of 58 users or about 20 users at each site

[b]Shared Medical Systems did not have pharmacy software operational at the time of our visit to Philadelphia

Users of the three commercial systems stated that (1) their system was generally available to them, though some had difficulty using it, (2) training generally was adequate, (3) they perceived the data in their system as accurate, and (4) their system helped them better perform their jobs (see appendix V for additional information). Twenty-seven medical center directors and managers who were interviewed also made similar favorable comments and concluded that their systems improved service to the veterans. According to detailed information obtained from vendors and VA officials, we found that both the commercial systems and DHCP offered many similar features

Test Structure Prevents Direct Comparison Between Commercial Test Systems and DHCP

Under congressional committee direction, VA was to analyze various alternatives, including commercial systems and VA's system, to determine which would be the most cost-effective and of maximum value to VA's medical center work. VA was directed to test commercial systems at three medical centers of varying sizes. However, VA did not structure or monitor the demonstration test to provide a reasonable comparison between the commercial systems and DHCP. For example:

- None of the demonstration test sites is in VA's larger medical centers. VA's largest medical center has 1,300 beds and the average size center has 500 beds. The test sites chosen (large, medium, and small, respectively) were Philadelphia, Pa., (419 beds); Saginaw, Mich., (158 beds); and Big Spring, Tex., (220 beds).
- The three vendors modified their own systems to meet site-specific needs without being required to address standard needs (for example, the same definitions of data to allow possible aggregation of data for

local, regional, and headquarters needs). Furthermore, the vendors' modifications were not reviewed and approved by headquarters.

At the vendors' request, VA extended the implementation deadline for mandatory functions by 1 year, from September 1985 to September 1986, to allow time for the vendors to modify their systems to meet local needs. Subsequently, the test was extended to September 1987, to allow time for the vendors to meet the terms of their contracts. In commenting on a draft of this report, VA stated that DHCP and the commercial test systems were originally conceived with different purposes and scope, "making comparison difficult but not impossible." VA stated that the three test sites do, in fact, represent a range of size and complexity. The agency added that different factors, in addition to the number of beds, are considered for projecting DHCP requirements. VA agreed that the commercial vendors were allowed to make site-specific changes to meet the specialized needs of VA users.

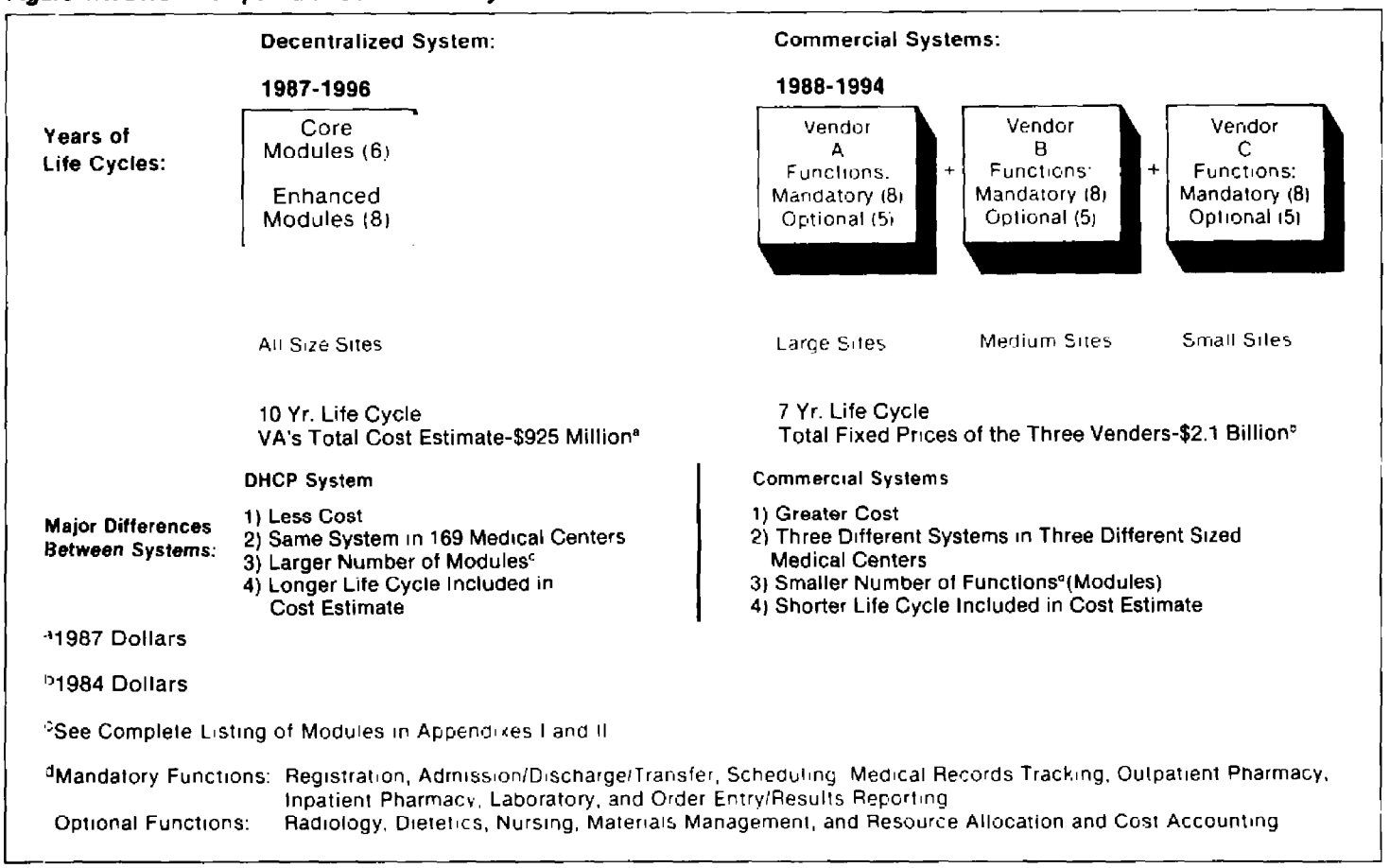
Under Contract Limitations, Commercial Test Systems Offer Fewer Features and Cost More Than DHCP

Each of the three vendors involved in the commercial demonstration test has a contract that cites the mandatory and optional functions to be tested and requests that a 7-year life cycle be used to estimate the costs of any installed systems. The contracts also preclude the installation of a single vendor's system in all VA facilities; rather, each vendor has a contract with the option to install its system in only one of three sizes of VA medical centers. This limitation makes it difficult to directly compare these systems with one another and with DHCP. This limitation also may cause the estimated costs of installing all three systems to be higher than installing one system throughout the agency.

Under current contract constraints, VA's commercial systems would cost more than the planned DHCP system. The commercial systems are designed to computerize VA's hospitals by providing software (some similar to DHCP modules) for eight mandatory and five optional functional areas over a 7-year life cycle for a combined cost of $2.1 billion in 1984 dollars. VA's currently planned DHCP system includes 14 modules over a 10-year life cycle for an estimated total cost of $925 million in 1987 dollars. Figure 4.1 illustrates the current differences between DHCP and the commercial systems.

The $2.1 billion collective price of the three vendors' fixed-cost contracts, however, does not include estimates for major costs that would be paid by the government. For example, if a vendor's system was implemented, VA would have to pay substantial costs for such items as

Figure 4.1: DHCP Compared to Commercial Systems



[a]1987 Dollars

[b]1984 Dollars

[c]See Complete Listing of Modules in Appendixes I and II

[d]Mandatory Functions: Registration, Admission/Discharge/Transfer, Scheduling, Medical Records Tracking, Outpatient Pharmacy, Inpatient Pharmacy, Laboratory, and Order Entry/Results Reporting
Optional Functions: Radiology, Dietetics, Nursing, Materials Management, and Resource Allocation and Cost Accounting

site preparation, telecommunications, utilities, and data base conversion. All of these costs plus others, such as related VA application coordinator staff support, interfacing two or more of the vendors' systems if more than one system is selected, and staff retraining, should be determined in comparing the cost of vendors' systems with DHCP's costs. A direct comparison between the systems would require that all costs for the commercial systems be considered and that they be compared with DHCP's life-cycle costs.

General Services Administration officials told us that VA cannot select one of these commercial systems for agencywide implementation under the original procurement authority it delegated to VA. This authority

only allowed the agency to acquire additional systems from the test vendors by exercising the contracts' fixed-price options. However, this delegated authority was limited to the options that VA evaluated for contract award and included in the vendors' contracts. The contracts VA awarded for the three demonstration tests included evaluated fixed-price options to install additional systems in only one of three sizes of medical centers: small, medium, or large. On the basis of the General Services Administration's Delegation of Procurement Authority, for VA to install one vendor's system at all of its centers, it would have had to include an option for this installation in the vendor contracts. Since the contracts were awarded without this option, it would now be necessary to obtain an additional Delegation of Procurement Authority to

- allow the agency to either recompete for a VA-wide system under a new contract, or
- award a new contract to one vendor on a sole-source basis after providing appropriate justification to the General Services Administration to warrant this decision.

These limitations resulted in vendors not offering discounts for larger quantity purchases or for cost savings that may be realized from an unrestricted optimal computer placement in all sizes of medical centers. For example, two vendors said that in many instances it may be less costly to use a regionalized approach, that is, a large computer center to serve several medical centers in one geographical area, rather than placing computers, along with supporting staff, in the individual hospitals. According to one vendor, the contract structure limited the vendor's ability to present more cost-effective alternatives, such as regionalized computer support.

In commenting on our draft report, VA agreed that the vendor contracts limited each vendor to installing its system in only one of three sizes of medical centers and that a new Delegation of Procurement Authority would be needed to install one vendor system in all VA medical centers. Officials said this limitation was based on the assumption that if a commercial package was successful at one center, it had the potential for successful implementation at a second facility of comparable size and complexity, but it would not necessarily be successful in centers that vary in size and scope from the contracted facility.

In January 1987, prior to VA's reducing the scope and estimated $1.2 billion cost of the DHCP system, two vendors told us that they may be

able to implement their systems VA-wide for less cost than the three combined bids in the vendor contracts, which total $2.1 billion. They gave us estimated ranges that they said depended upon the type of hardware configuration used. One vendor estimated its system would cost from $930 million to $1.45 billion for a 7-year life cycle, but qualified the estimate by stating that it was not a fixed-price proposal and that additional costs might be incurred. The second vendor's gross estimate for its system was $1.7 billion to $2.1 billion for a 9-year life cycle, which would take 3 to 5 years to fully install. However, neither of the vendors provided detailed documentation to support their proposed estimates. Another vendor said that it would cost as much as $100,000 to prepare an appropriate proposal.

In February 1987, a consulting firm, Booz-Allen & Hamilton, Inc., issued a comparability study[2] that presented a strategic assessment of the cost-effectiveness of the DHCP and commercial systems. The study made assumptions to adjust both DHCP and the vendors' systems to a 10-year life cycle and concluded that DHCP was the least costly system. After receiving the consultant's report, VA decided to continue with DHCP and not to implement any of the three commercial test systems at other VA sites. A Management Office official said that after he receives another consultant's report on the demonstration test in September 1987, VA will make further decisions about the vendors' systems at the three medical centers. He said that, to avoid unnecessarily disrupting these facilities, VA expects to phase out the systems over at least a 1-year period. However, when commenting on a draft of this report, VA stated that now it has no specific plans to phase out the commercial systems and that the vendor will be expected to continue operating these systems throughout fiscal year 1988. Using the commercial systems in place of DHCP would require removing DHCP at 169 medical centers (a total of 225 facilities), disrupting the medical centers' operations, retraining staff, incurring costs to change to the vendor's equipment, paying for the use of proprietary software, converting data from the DHCP data base to the vendor's system, and the commercial systems would have a shorter life cycle with fewer functions.

In commenting on our draft report, VA stated that it revised the DHCP cost estimates to include additional factors we had identified and asked

[2]Decentralized Hospital Computer Program and Integrated Hospital System Comparability Study (Booz-Allen & Hamilton, Inc., Bethesda, Maryland, February 1987)

Booz-Allen to do the same for its comparability study. The agency concluded that the revised estimates showed that both DHCP and the commercial systems would cost more than previously estimated, but that the commercial systems were significantly more expensive than DHCP. According to VA, the commercial systems test "was not intended as a vehicle for comparing commercial systems to DHCP." However, the agency said that, although a comparison was difficult, it was not impossible and that Booz-Allen was able to "normalize" key cost and effectiveness elements, between the 10-year, 14-module DHCP system and the three commercial systems and compare these two computerization approaches.

Although Booz-Allen's comparison showed that DHCP was less costly than the commercial systems ($925 million versus $1.6 billion in 1987 dollars), this analysis was based on several major assumptions. For example, according to VA and Booz-Allen, to make the 10-year cost comparison, Booz-Allen had to (1) increase the commercial system life-cycle cost from 7 to 10 years, (2) identify 17 generic functions for DHCP and assume that 3 of these functions not addressed in the commercial system contracts would be available in the marketplace, and (3) assume that a single nationwide contract would account for economies of scale in estimating the life-cycle cost of the commercial systems. The difficulty of making an adequate comparison under these assumptions is emphasized by the fact that VA agreed with us that it did not intend to use the test to compare the commercial systems with DHCP and that, under the commercial contracts, individual vendors cannot install their individual system nationwide; thus, they cannot utilize the economies of scale.

In addition to the difficulty of making an adequate cost comparison, the Booz-Allen study was also based upon the assumption that both the DHCP and commercial systems would use a decentralized configuration with computers at each hospital site. In commenting on our draft report, VA said that the vendors' assertion that they could provide computer services nationally to VA at less cost if they used regionalized computer hardware to serve multiple facilities was not relevant. VA stated that:

"Use of regional computers for local operations is not acceptable to the VA. Moreover, in the unlikely event that local performance and response requirements could be met without driving telecommunications costs to unacceptable levels, such regionalization could be achieved in-house through DHCP. It is, therefore, not useful in any discussion of DHCP versus IHS [the commercial systems]."

However, VA provided no empirical evidence to support this position.

As we described in chapter 3, VA cannot be assured it has selected the most cost-effective system until it considers other configuration approaches. Similarly, VA would need to allow commercial vendors to select their optimum configuration to be assured of the most cost-effective commercial alternative.

Conclusions, Recommendations, and Agency Comments and Our Evaluation

Conclusions

VA has made significant progress in providing computer support to its medical centers through the DHCP system. By allowing decentralized development and implementation of this system, VA successfully achieved user participation and acceptance, which contributed to a timely and successful implementation of the initial phase. However, because this approach received only informal direction from a central authority, it resulted in software development that did not follow federal guidelines to appropriately document, test, and approve the software before it was released. Without such controls, software was developed that (1) was prematurely released requiring multiple corrections and (2) is susceptible to undetected errors. Lack of such controls also makes it difficult to assess whether appropriate software changes have been or should be made.

The decentralized development approach also resulted in inadequate controls by (1) not requiring that risks to computer data, equipment, and facilities at the medical centers be assessed and (2) not requiring that computer development and operations staff hold appropriate levels of security clearance. Furthermore, because VA released its software (including security information) under the Freedom of Information Act, private sources might have been able to use this software for unauthorized access to VA's patient data. These conditions put sensitive patient data at risk of improper disclosure, destruction, or inappropriate alteration and may adversely affect VA's ability to provide high-quality health care. We believe the lack of such controls are material weaknesses under the Federal Managers' Financial Integrity Act. VA has recognized these problems and begun to take corrective actions.

VA is beginning a $385 million expansion of DHCP that if completed, has a VA-estimated total life-cycle cost of $925 million for the 6 Core and 8 Enhanced modules. With an investment of this magnitude, it is incumbent on VA to effectively plan and manage the expansion to ensure that the system fulfills its objectives cost-effectively. However, VA has selected a decentralized hardware configuration with on-site computers for DHCP and has determined that other configuration alternatives, such as a regionalized system, are not acceptable. While these alternatives may meet VA's needs at less cost, without explicitly evaluating other hardware configuration alternatives VA has no assurance that the most cost-effective approach will be used. Although other alternatives may be feasible and more cost-effective, VA has determined that the need to use a decentralized configuration to meet its local management and control objectives is an overriding issue.

VA's expansion plans also include procuring over $84 million in computer hardware and installing computers based on a sizing model. However, without obtaining and considering data on existing computer utilization and available capacity, VA cannot be certain the planned equipment acquisitions are appropriate because it may be understating or overstating the equipment requirements at individual medical centers that are not accounted for in the model.

Regarding VA's demonstration test of three commercial systems, the test's structure and the contract limitations prevent VA from making a direct comparison between the commercial systems and DHCP. The test structure did not evaluate the commercial systems at representative sites, nor did it ensure that the development of systems was comparable to DHCP and that they would meet VA needs agencywide. The test contracts' limitations resulted in vendors' proposing estimates for installing systems (1) that had shorter life cycles and fewer features than DHCP, and (2) that could not take into consideration the economies of scale by installing a vendor system in all VA medical centers. VA's consultant made several assumptions to compare the DHCP system with the commercial test systems. On the basis of the consultant's report, VA has concluded that it would be more costly to use a commercial system than the DHCP system.

As VA embarks on an expansion of DHCP, it is critical that VA exercises the management control necessary to ensure that the expansion fulfills its objectives cost-effectively. VA's recent changes to provide its Management Office with authority to control the future development and implementation of DHCP is a positive step. Office policies and procedures that will direct and monitor future efforts are necessary for successful DHCP implementation.

Recommendations

We recommend that the Administrator of Veterans Affairs report the lack of sufficient software development controls and continue to report the lack of risk analyses and contingency plans as material control weaknesses under the Federal Managers' Financial Integrity Act until (1) appropriate software development controls have been implemented, (2) risk analyses (as well as needed corrective action identified by such analyses) have been completed for all computer centers, and (3) contingency plans have been developed, certified, and tested.

Moreover, the Administrator should hold the Management Office, under its recently increased authority, accountable for ensuring that the

existing and expanded DHCP system is effectively managed and adequately protected. At a minimum, this office should

- institute procedures to collect work load and cost/benefit data on prototype modules at test sites to assist in determining incremental hardware requirements and developing cost/benefit analyses;
- implement controls to ensure that software is adequately tested, documented, and approved, and that software and hardware problems are systematically tracked and corrected;
- implement appropriate internal controls to protect data, equipment, and facilities as required in OMB Circular A-130 and further provided for in the Federal Information Processing Standards Publication 31;
- issue a policy to restrict release of DHCP software (including security information) under the Freedom of Information Act in order to protect sensitive patient data;
- ensure that data requirements are defined and incorporated in the DHCP modules so that the data can be efficiently accessed by system users; and
- establish policy and procedures for regularly monitoring system utilization and assessing computer capacity VA-wide to better determine hardware requirements.

Agency Comments and Our Evaluation

On June 5, 1987, VA provided written comments on a draft of this report (see appendix VI). It agreed that we had identified a number of significant problems and said that in general, it had already noted and moved to resolve them. VA also commented that discussions between GAO and VA staffs throughout the review had served to focus VA's attention on problem areas and helped it to identify solutions. Since VA agreed with our recommendations in these areas and has already acted on them, we have made changes throughout the report to reflect the corrective action taken or in process by VA.

However, the agency did not concur with one major recommendation in the draft report—that the Administrator of Veterans Affairs take the necessary steps to ensure that adequate information is developed for making sound decisions before proceeding with the planned expansion of DHCP. We stated that this information should include, at a minimum, a comprehensive and accurate life-cycle cost estimate and cost/benefit analysis that considers various system design alternatives as called for in federal regulations and guidelines and that these analyses include a commercial system approach. We made this recommendation because we

believed the potential for cost savings warranted the recommended action.

In responding to our draft report, however, VA stated that it had selected a decentralized hardware configuration alternative with on-site computers and that other alternatives, such as a regionalized approach, were unacceptable. VA stated that it had "rejected a regionalized systems approach because it compromises critical aspects of the DM&S [Department of Medicine and Surgery] information management program" and would not allow hospital managers to have adequate control and responsibility over their systems. VA added that in its original cost/benefit analysis and in the current one, the comparison is between continuing to automate through DHCP and maintaining a manual system. VA officials added that, "We did not consider a regional configuration because the purpose was to determine whether to extend the existing decentralized system." VA indicated that taking time to explicitly evaluate other alternatives would adversely affect its computerization effort and ultimately its service to veterans. It added that an additional alternative system design analysis was not needed because this area had been, "implicitly evaluated and determined not to be cost-effective for providing computer support to VA medical centers," particularly because of increased telecommunications costs.

VA also said it was not necessary to compare DHCP with a commercial system as part of the cost/benefit analysis because it had commissioned a major cost-effectiveness study to compare a commercial systems approach with DHCP and found that the commercial systems approach was significantly more costly than DHCP. The agency concluded that

> "This information, along with all the other information that we have supplied, is evidence that VA has taken all necessary actions to ensure that it meets its computerization needs in a cost-effective manner. Congressional funding should not be limited because that would deprive VA medical providers of an essential tool in delivering quality care to eligible veterans."

VA's response included a description of areas where a "regionalized" system design with remotely located computers can be more costly, inefficient, and nonresponsive to users than a decentralized system. However, VA did not perform a detailed analysis to support its conclusion nor did it assess the potential cost savings in such areas as hardware, site preparation, and personnel. Because VA's current $925 million, 10-year-life-cycle, 14-module system has fewer features, it has a higher proportional cost than the system planned in 1986. Thus, increased emphasis is

placed on the need to evaluate alternatives and select the most cost-effective approach.

Matter for Congressional Consideration

VA has implemented the DHCP Initial Core modules with resultant user satisfaction and expects to completely implement the Full Core modules by the end of 1987 to support its critical information needs throughout its medical centers. Thus, since the most critical needs should be met in 1987, we believe the opportune time to consider the feasibility of potential alternatives would be now, before VA initiates a major investment to enhance its DHCP system. However, VA believes that a decentralized configuration is needed to meet its local management and control objectives and that the consideration of other alternatives could adversely affect service to veterans. The Congress must ultimately decide whether the issues raised by VA justify its not explicitly considering potentially more cost-effective system design alternatives in meeting VA's medical computerization needs. We believe the information in this report should assist the Congress in reaching future funding decisions on this program.

Description of VA's DHCP Initial and Full Core Modules

Initial Core

The four Initial Core modules include: patient registration, admission/discharge/transfer, clinic scheduling, and outpatient pharmacy. Computerizing this data allows VA medical center staff to access the most current information on the demographics and location of each patient as well as the medications prescribed for each veteran.

Registration

This module is used to register the patient for treatment at the medical center and makes the demographic information on each patient available to all system users throughout the medical center. The demographic data include the patient's name, address, social security number, and eligibility for medical care.

Admission/Discharge/Transfer

This module supports the functions that make it possible for medical center staff to admit, discharge, transfer and track patient status/location, generate patient gain and loss statistics, and produce bed census reports and ward rosters.

Clinic Scheduling

This module is used to schedule both inpatients and outpatients for clinic appointment visits; track all appointments for a given patient in different clinics; eliminate duplication of patient appointments, travel expenditure, and meal claims; generate file room "pull" data; identify patients that do not show up for their appointments; and send pre-appointment and clinic cancellation letters to outpatients.

Outpatient Pharmacy

This module provides control of drug data for the medical center's outpatients, allows staff to check drug interactions, maintains patient medication profiles, produces prescription labels, contains a submodule to maintain specific drugs in the pharmacy formulary (a book containing a list of medical substances and formulas), and generates related management information.

Full Core Modules

Full Core software adds clinical laboratory and inpatient pharmacy modules to the Initial Core DHCP environment. This software is integrated with the Initial Core modules to complete support for the recognized areas of "critical" need.

Clinical Laboratory

This module is a comprehensive, integrated laboratory computer system. The module includes submodules to support chemistry, hematology, microbiology, anatomic pathology, and blood bank (these submodules are not implemented at all sites). This software permits the ward to order laboratory tests and receive the results. Test results can be routed to several different locations. A patient laboratory profile is maintained to augment the patient records. In addition, it allows the order entry and tracking of requests for tests, and provides collection lists and labels for blood collection, accessioning of specimens into the laboratory, and work lists of tests to be performed. The module facilitates the entry of data, both manually and via interfaces, to automated instruments; generates reports for review and quality assurance; produces various reports providing timely and accessible review of patient data; and produces reports to physicians on patients.

Inpatient Pharmacy

This module supports several different dispensing methods in three submodules, including unit doses, ward stock, and intravenous additives. The module contains many of the same capabilities as the outpatient pharmacy module, such as maintaining current medication profiles (for inpatients), allowing staff to check for drug interactions, and providing management information reports. In addition, this module enables drugs to be ordered for inpatients on the medical center wards, provides profile reviews in a variety of medical center locations, tracks returned or non-administered drugs, and provides intravenous solution management.

Development Status of Currently Planned DHCP Enhanced Modules

DHCP Enhanced Modules by Priority	Available	Scheduled Implementation
1 Radiology	Yes	1987
2 Dietetics	Yes	1987
3. Medical Records Tracking	Under development	1987
4 IFCAP (Fiscal & Supply)	In Beta test[a]	1987
5 Decentralized Medical Management System	Under development	1988
6 Surgery	In Beta test[a]	1988
7 Mental Health	Yes	1989
8 Nursing	In verification[b]	1989

Note: The planned order entry/results reporting feature discussed in chapter 3 is a DHCP systemwide "utility" package and is not a stand-alone application in the Enhanced module priority list. Three of five planned components are available, and the others are under development.

[a]Prototype development of each DHCP application module is performed in a medical facility designated as an Alpha test site. A subsequent Beta test is performed at another site(s) to evaluate the software in a production environment.

[b]Following the Beta test, the software is verified for both technical and functional adequacy by an Information Systems Center, other than the center that developed the software.

Previously Planned Enhanced and Comprehensive Modules That Now Are Not Included in the DHCP System

Modules by Priority	Status as of June 1987 When the Scope of the DHCP Program Was Reduced
Enhanced	
1. Management Support	Under development
2. Medicine	Under development
3. Department of Veterans Benefits Interface	Available
4. Fee Basis	Under development
5. Social Work	Available
6 Engineering	Available
7 Dentistry	Available
8. Rehabilitation Medicine	Under development
9 Extended Care/Geriatrics	Under development
10 Nuclear Medicine	Planned
11. Personnel	Under development
12. Readjustment Counseling/Outreach	Planned
13. Operating System Enhancements	Under development
14. Message Handling/Switching	Under development
Comprehensive	
1 Audiology and Speech Pathology	Planned
2 Prosthetics	Under development
3 Orthotics	Planned
4 Optometry	Planned
5. Podiatry	Planned
6. Library Service	In Beta test
7. Medical Media	Planned
8. Building Management	Planned
9. Voluntary Service	Planned
10. Recreation Service	Planned
11. Chaplain Service	Planned
12 Canteen Service	Planned
13. Gastroenterology	Planned
14 Oncology	Under development
15 Neurology	Planned
16 Pulmonary Service	Planned
17 Patient Monitoring	Planned
18 Pacemaker Registry	Under development
19 Space Management	Planned

(continued)

Modules by Priority	Status as of June 1987 When the Scope of the DHCP Program Was Reduced
20. Employee Health	Planned
21 Parking Management	Planned
22. Security/Police Service	Planned
23 Research Administrative Support	Under development

Note On June 5, 1987, VA told us that the scope of the DHCP system had been reduced to include only the six Core and eight Enhanced modules shown in appendixes I and II According to VA the Enhanced and Comprehensive modules listed above are now only "potential areas for future automation " A VA official said that these modules are no longer under development and that their inclusion in the DHCP system would be based on the outcome of future cost/benefit studies.

Criteria for Developing Full Cost Estimates

	Available Guidelines			
Cost Elements	**Fed. Pub. 64[a]**	**Circular No. A-121[b]**	**Circular No. A-130[c]**	**Circular No. A-11[d]**
Personnel	X	X	X	X
Salaries	X	X	X	X
Overtime		X	X	X
Fringe Benefits	X	X	X	X
Training	X	X	X	X
Travel	X	X	X	X
Equipment	X	X	X	X
Purchase of Hardware	X	X	X	X
Depreciation for Owned Capitalized Equipment		X	X	
Equipment Rental or Lease	X	X	X	X
In-house Maintenance	X			
Data Communication Equipment	X			
Environment Conditioning Equipment	X			X
Security and Privacy Equipment	X			
Direct Expenses for Noncapitalized Equipment		X	X	
Special Purpose ADP Furniture				X
Software	X	X	X	X
Depreciation for Capitalized Costs of Developing, Converting or Acquiring Software		X	X	
Rental Costs	X	X	X	X
Direct Expenses for Noncapitalized Acquisition of Software		X	X	
Lease Costs	X			X
In-house Maintenance	X			
Software Conversion	X			
Purchase Price				X
Supplies	X	X	X	X
Office Supplies		X	X	
Data Processing Materials		X	X	
Miscellaneous Expenses		X	X	
Contracted Commercial Services	X	X	X	X
Technical Consulting Services	X	X	X	
Equipment Maintenance		X	X	X

(continued)

Cost Elements	Available Guidelines			
	Fed. Pub. 64[a]	Circular No. A-121[b]	Circular No. A-130[c]	Circular No. A-11[d]
Operations Support		X	X	X
Maintenance of Software (Operating System, Multipurpose, and Application Software)		X	X	X
Telecommunications Network Services/Data Communications	X	X	X	X
Facilities Management			X	X
Advice on Acquisition Selection and Use of Computer Facilities or Software				X
Data Entry Support		X	X	X
Analysis, Design, Programming, Documentation, Modification, and Testing for Development Conversion and Upkeep of Computer Software				X
Space Occupancy	X	X	X	X
Rental, Lease, and Depreciation of Buildings, General Office Furniture, and Equipment		X	X	X
Heating, Air Conditioning, and Other Utilities Expenses	X	X	X	X
Telephone Charges		X	X	
Power-Conditioning and Distribution Equipment and Alternative Power Sources			X	X
Rehabilitation, Modification or Addition of Land/ Building				X
Site Preparation/ Construction	X			X
Building Maintenance		X	X	
Security and Custodial Services		X	X	X
Intra-Agency Services and Overhead	X	X	X	X
Costs of Normal Agency Support Services		X	X	
Inter-Agency Services	X	X	X	X
Other Security and Privacy Services	X			
Requirement and Design Studies	X			
Procurement Planning and Benchmarking	X			
Reviews and Other Technical and Management Overhead	X			

(continued)

Cost Elements	Available Guidelines			
	Fed. Pub. 64[a]	Circular No. A-121[b]	Circular No. A-130[c]	Circular No. A-11[d]
Data Base and Data Base Preparation	X			
Incremental or Additional Overhead Costs	X			

[a]Federal Information Processing Standards Publication 64, "Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase," August 1, 1979

[b]Office of Management and Budget Circular Number A-121, "Cost Accounting, Cost Recovery and Inter-Agency Sharing of Data Processing Facilities," September 16, 1980

[c]Office of Management and Budget Circular Number A-130, "Management of Federal Information Resources," December 12, 1985

[d]Office of Management and Budget Circular Number A-11, "Preparation and Submission of Budget Estimates," May 28, 1986

Commercial-System Users Interviewed Were Satisfied With Vendor Systems[a]

Percentage of users

User Satisfaction Factors	Philadelphia	Saginaw	Big Spring
System availability			
Response time was 4 seconds or less	82	89	70
Response time had occasional/no effect on efficiency	76	83	87
Terminal malfunction was no problem	82	67	70
Ease of use			
Data were easy to enter	94	78	83
Processing large volumes of data was no problem	75	62	40
"Help" messages were clear	94	83	56
Training			
Local training was adequate	82	94	100
Data accuracy			
Data in system were accurate	94	94	87
System successfully limited data entry errors	82	44	39
Performance			
System helped job performance	71	72	52

[a]Based on interviews with a total of 58 system users, about 20 users at each site.

Agency Comments

Office of the Administrator of Veterans Affairs

Washington DC 20420

Veterans Administration

JUN 5 1987

Mr. Charles A. Bowsher
Comptroller General of the United States
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Bowsher: Charles,

Thank you for the opportunity to review your April 20, 1987, draft report Hospital ADP Systems: VA Needs to Better Manage Its Decentralized System Before Expansion. The Decentralized Hospital Computer Program (DHCP) has become an essential tool to VA medical practitioners as they go about their daily work of providing care to our nation's veterans, and I appreciate both the care and the technical expertise that your staff brought to this study.

It is significant you found that users in general indicated that the system met their needs for critical information, was accurate and easy to use, helped them do their jobs better, and provided the flexibility needed in a computer system. This is certainly what staff have told me in my many visits to our medical centers.

However, you also identified a number of significant problems. In general, these are problems we have already noted and moved to resolve. In fact, the discussions our staffs have had over the last 2 years while your report was being prepared often served to focus our attention on problem areas and helped us to identify solutions.

The first management decision I took concerning DHCP was that all additional applications would be subject to a cost-benefit analysis which weighed the costs of the new applications against the benefits--both qualitative benefits that result in improved patient care and quantitative benefits that lower costs and increase productivity. For this reason, it is now inappropriate to speak, as your report does, about 53 modules. As you know, equipment for Core has already been purchased, Initial Core is fully implemented, and Full Core will be implemented by the end of the calendar year. In addition, eight Enhanced DHCP applications have met the Office of Management and Budget investment criteria and been approved: Radiology, Dietetics, Medical Records Tracking, IFCAP (Integrated Funds Control/Control Point Activity/Accounting and Procurement), Surgery, Decentralized Medical Management System, Nursing, and Mental Health. Life cycle costs relate only to these applications (sometimes referred to as "Core plus eight").

JUN 5 1987

2.

Mr. Bowsher, Comptroller General

We have attempted to develop life cycle costs for Core plus eight that are as comprehensive and accurate as possible. However, your staff have identified certain costs that were omitted and we have revised the costs, as described in Enclosure 2, to rectify these omissions. At the same time, Booz-Allen and Hamilton, who developed the costs for the Integrated Hospital System (IHS), the commercial alternative, also reviewed their costs and revised them as necessary. According to these revised costs, the 10-year life cycle cost of DHCP, beginning in fiscal year 1987, is between $878 million and $925 million (depending on the fringe benefit rate); the comparable cost for IHS is between $1,587 million and $1,596 million. I believe that this cost comparison makes a strong case for DHCP. Enclosure 3 is the May 29, 1987, letter from Booz-Allen updating their DHCP IHS cost comparison.

As noted above, I approved the eight priority applications for Enhanced DHCP only after a cost-benefit analysis by the national accounting firm Price Waterhouse showed that the investment was justified. In light of the criticisms in your report and in order to take account of the revised cost estimates, we asked Price Waterhouse to update their analysis. The new analysis shows a net rate of return of 9 percent to the taxpayer. The rate of return to the VA is 6.4 percent. These rates of return are calculated on the basis of quantifiable savings only. There are also significant improvements in the quality of services provided and these are described in the Price Waterhouse report (Enclosure 4). Their report confirms my original judgment that the equipment for these Enhanced DHCP modules is a good investment that will benefit both the veteran and the taxpayer.

The Price Waterhouse analysis makes the comparison between DHCP and maintaining the current manual mode of operations in these areas. We never asked Price Waterhouse to compare DHCP with a commercial alternative because we were doing a congressionally mandated cost-effectiveness study comparing DHCP with the Integrated Hospital System, a commercial alternative that we had been testing at three sites. I believe this study by Booz-Allen and Hamilton fully satisfies the requirement that we consider a commercial approach as an alternative and the results are unambiguous: DHCP is significantly less costly.

Your report also notes that the program's shortcomings exist largely because the office responsible for managing DHCP did not have the necessary authority to manage development and implementation. I fully agree. In February 1987, I approved a reorganization giving the Medical

JUN 5 1987

3.

Mr. Bowsher, Comptroller General

Information Resources Management Office (MIRMO) the authority it needs to manage the program effectively. I am pleased to tell you that we are already seeing the results of this change:

-- Verification policies have been established so that software is fully tested before release, software releases are technically correct, and software documentation is complete and correct.

-- Procedures have been established providing for program office sign-off on software prior to national release, thereby ensuring that it meets program needs and conforms to national policy.

-- Work is underway to improve risk analysis and contingency planning. A number of significant changes in software have already been made, for example, ensuring that patients' eligibility can be altered only by properly authorized individuals, that only properly authorized individuals access the system, and that these individuals are given limited access on a "need to know" basis.

-- Work is underway to improve, formalize, and streamline software and hardware tracking.

-- Policy for releasing software under Freedom of Information Act requests has been reviewed and confirmed to ensure that sensitive information, such as security algorithms, is not released.

-- Work has been accelerated on the Order Entry/Results Reporting package to enhance results reporting features.

These and other actions are discussed more fully in the enclosures. Our comments on the recommendations appear in Enclosure 1. Enclosure 2 provides our comments on the text of your draft report.

In summary, DHCP is a cost-effective program that serves the needs of our medical centers and the veterans whom we treat. Both the cost-effectiveness analysis comparing DHCP with IHS and the cost-benefit analysis unambiguously support our decision to continue with DHCP. In the draft report, you acknowledge that the problems observed in the course of your study have either been corrected or are well on the way to resolution. VA is committed to a dynamic process of examining our assumptions, refining our estimates, and checking their validity through

JUN 5 1987

4.

Mr. Bowsher, Comptroller General

postimplementation evaluations. It would be a mistake to limit funding. It would demoralize staff in the medical centers; cause programmers and other key ADP personnel to leave; and deprive medical center staff of a proven, cost-effective tool. Our efforts would be better spent working together to make the DHCP program even better than it already is rather than doing yet another study. Our veterans deserve the improvements in efficiency and quality of care that DHCP will give them.

Thank you for the opportunity to comment on your draft report. Please publish this letter and the first three enclosures with your final report.

Sincerely,

THOMAS K. TURNAGE
Administrator

Enclosures 4

Enclosure 1

VETERANS ADMINISTRATION COMMENTS ON THE RECOMMENDATIONS IN THE APRIL 20, 1987 GAO DRAFT REPORT "HOSPITAL ADP SYSTEMS: VA NEEDS TO BETTER MANAGE ITS DECENTRALIZED SYSTEM BEFORE EXPANSION"

GAO recommended that the Administrator of Veterans Affairs take the necessary steps to ensure that adequate information is developed for making sound decisions before proceeding with the planned expansion of DHCP. This information should include, at a minimum, a comprehensive and accurate life-cycle cost estimate and cost-benefit analysis that considers various system design alternatives as called for in federal regulations and guidelines. The alternative analyses should include a commercial system approach.

Concur. Enclosure 2, page 13, contains a revised life cycle cost estimate for all DHCP applications currently planned and approved (CORE plus eight) that includes those items which had been improperly omitted. It has also been updated to include more current information. The specific revisions are explained in our comments on Chapter 3. (See Enclosure 2.) The revised cost-benefit analysis, prepared by Price Waterhouse, follows federal regulations and guidelines and is provided as Enclosure 4. As explained in the comments on Chapter 3, it does not include a commercial system approach because that was the object of a separate cost-effectiveness analysis by Booz-Allen and Hamilton. That analysis showed that it would cost $1,595,838,000 under the Integrated Hospital System (IHS) (a commercial system) to achieve the same level of effectiveness that could be achieved for $924,880,000 under DHCP.

To assist in determining incremental hardware requirements and developing cost-benefit analyses, the Administrator should ensure that the Management Office institutes procedures to collect cost and benefit data on prototype modules at test sites.

We do not believe that it would have been cost-effective to collect new cost and benefit data at prototype sites. The methodology used here--a prospective cost-benefit analysis in which benefits were based on an assessment by program experts of the fuctionality of the modules and their anticipated impact--was selected in preference to a methodolgy requiring new data collection. However, both costs and benefits are under continuing review and analysis, and the cost-benefit analysis will be validated by postimplementation evaluations of all modules.

We believe a mathematical model that incorporates parameters describing clinical and administrative workload on a medical center-specific basis, as well as estimates of the capacity required to support the functionality incorporated in each application, is the best way to develop systemwide equipment requirements. The model receives input from Information Systems Centers (ISC's) and software developers who draw upon their knowledge of the application functionality as well as on alpha and beta test site experience. However, simple extrapolation from experience at a handful of test sites is not sufficient because test sites, no matter how carefully chosen, cannot fully represent the range of all medical centers' workload and because the mix of applications implemented must be taken into account, particularly in estimating central processing unit capacity. Because the model projects

2.

workload related to Core as well as the eight enhanced applications (i.e., a zero-based, not marginal projection), it is not important to empirically measure each computer configuration's current workload to get accurate projections of sizing. In fact, a redistribution of current capacity is called for by the output. We will continue to develop and refine the DHCP sizing model, incorporating new prototype results as they become available. We do not believe that any other approach is feasible.

Also, the Administrator should report the lack of software development controls and continue to report the lack of contingency plans and risk analyses as material control weaknesses under the Federal Managers' Financial Integrity Act until (1) appropriate software development controls have been implemented, (2) contingency plans have been developed, certified, and tested, and (3) risk analyses (as well as needed corrective action identified by such analyses) have been completed for all computer centers.

Concur. As indicated in the report, the Medical Information Resources Management Office (MIRMO) issued an interim directive in December 1986, setting forth detailed policies to ensure that software is thoroughly tested before release, that software releases are technically correct, and that supporting documentation is both complete and correct. We expect to issue these guidelines as a formal circular in October 1987. In the meantime, the ISC's, which now report to MIRMO, are held accountable for compliance with this policy.

The December 24, 1986, Special Interest Users Group (SIUG) Circular 10-86-147 provides for program office sign-off on software before national release, thereby assuring that the package is functionally acceptable and conforms to national program policies.

Risk analysis and contingency planning were both addressed in the 1985 Department of Medicine and Surgery Security Circular 10-85-116. We agree that this circular did not provide enough guidance to sites for comprehensive risk analyses of automated systems. Consequently, the thoroughness of risk analysis and contingency planning varied from site to site. A new circular has been prepared and is under review, with a target release date of October 1987. The new circular will mandate contingency planning and will include a generic risk assessment questionnaire for facilities' use. It will result in a more consistent and thorough approach to risk analysis and contingency planning throughout the system.

Moreover, the Administrator should hold the Management Office, under its recently increased authority, accountable for ensuring that the existing and expanded DHCP system is effectively managed and adequately protected. At a minimum, this office should

- **-- establish controls to ensure that software is adequately tested, documented, and approved, and that software and hardware problems are systematically tracked and corrected;**

Concur. MIRMO is now fully accountable for the effective management and full protection of the current and future DHCP system.

3.

The controls that have been established to ensure the adequate testing, documentation, and approval of software are discussed in Enclosure 2. Multiple mechanisms are used for tracking hardware and software problems. Computer hardware problems are tracked jointly by the site manager, local vendor representatives, and the responsible Information Systems Center. Each ISC is also responsible for tracking the frequency of hardware/software problems for stations under their jurisdiction and reporting them to the contracting officer's technical representive (COTR), an ISC Director who has been given this national responsibility. In this way, problems that are common to multiple sites are identified for solution by the COTR. Information on common problems and their solutions is distributed nationally through electronic mail. Operating system problems are reported via electronic mail to the COTR, who contacts the vendor, resolves the problem, and reports the solution to the field.

Application software problems are generally reported through electronic mail, where they are tracked by both the developing ISC (which is responsible for their resolution) and MIRMO. Centralized software fixes are posted on the national patch system that all sites access through electronic mail.

Although these procedures have proven effective, we believe they should be formalized, improved, and streamlined. We are currently evaluating the specifications for a uniform national tracking system to report and track software/hardware problems and their solutions.

(The Management Office should) implement appropriate internal controls to protect data, equipment, and facilities as required in OMB Circular A-130 and further provided for in the Federal Information Processing Standards (FIPS) Publications 38 and 64;

Concur. As discussed above, we believe that the new security circular, that mandates contingency planning and includes detailed procedures and tools for risk assessment, will substantially improve internal controls and place DHCP in full compliance with OMB Circular A-130 and the guidelines of FIPS 38 and 64.

(The Management Office should) reassess its current policy regarding the unrestricted release of software (including security information) under the Freedom of Information Act (FOIA) in order to protect sensitive patient data;

Concur. In June 1986, the Chief Medical Director asked the General Counsel to review whether the Freedom of Information Act requires release of all DHCP software, including internal controls and security algorithims. In November 1986, the General Counsel ruled that existing FOIA exemptions permit withholding security-sensitive portions and algorithms from public release. We are now following the November 1986 ruling, and a circular setting forth this policy is in concurrence.

(The Management Office should) define data requirements and ensure that they are incorporated in the DHCP modules so that the data can be efficiently accessed by system users;

4.

Concur. So that the DHCP integrated data base can be used most efficiently, the Director of MIRMO has made development of the Order Entry/Results Reporting Options (OE/RR) module the highest priority of the Information Systems Centers. This utility will have a number of features that enhance current OE/RR capabilities. The most important of these will be a results reporting function that allows the user to access patient data originating in various modules with a single keystroke and display them on a single screen. This utility will be available for beta testing this summer.

(The Management Office should) establish policy and procedures for regularly monitoring system utilization and assessing computer capacity VA-wide to better determine hardware requirements.

Concur. MIRMO is currently working, through a contractor, on a tracking system that will maintain an accurate inventory of computer equipment/capacity at each of the medical centers as well as up-to-date information on utilization, especially implementation of national packages. One of the uses of this system will be to provide a validation of sizing model estimates and information with which to refine the model. We are also working through the ISC's to assist the medical centers in more effectively configuring their systems to obtain maximum efficiency. As the report notes, an interagency agreement with the Federal Computer Performance Evaluation and Simulation Center (FEDSIM) will provide technical support in configuration management and capacity planning.

Matter for Congressional Consideration

To ensure VA meets its computerization needs in a cost-effective manner, congressional funding should be limited, contingent on the Agency making satisfactory progress in developing a comprehensive and accurate life-cycle cost estimate and cost/benefit analysis that considers various system design alternatives.

As part of this response we are providing a comprehensive and accurate life-cycle cost estimate that takes account of the criticisms made by GAO. We are also attaching an updated cost/benefit analysis, prepared by Price Waterhouse, that uses the new life cycle costs and follows the guidelines of FIPS Publication Number 64. We contracted with Booz-Allen and Hamilton to do a cost-effectiveness study comparing DHCP with the Integrated Hospital System. Their study has been made available to GAO, and this response includes Booz-Allen and Hamilton's revised cost-effectiveness estimates that incorporate adjustments made in response to GAO's criticisms to both DHCP and IHS costs.

This information, along with all the other information that we have supplied, is evidence that VA has taken all necessary actions to ensure that it meets its computerization needs in a cost-effective manner. Congressional funding should not be limited because that would deprive VA medical providers of an essential tool in delivering quality care to eligible veterans.

Enclosure 2

VETERANS ADMINISTRATION COMMENTS ON TEXT OF
GENERAL ACCOUNTING OFFICE APRIL 20, 1987, DRAFT REPORT
"HOSPITAL ADP SYSTEMS: VA NEEDS TO BETTER MANAGE ITS
DECENTRALIZED SYSTEM BEFORE EXPANSION"

CHAPTER 1: INTRODUCTION

The introduction to the GAO report contains a factual presentation of the history of the Decentralized Hospital Computer Program (DHCP) and the Integrated Hospital System (IHS) pilots.

We would like to expand on the VA view of an integrated information system which appears in footnote 2. We view a fully integrated system as one that uses common file structures, common data files, common system utilities and a common user interface. All DHCP systems, for example, use a common data dictionary; common data base management system (the VA File Manager); common menus; and common programs, packages, functions, documentation, displays, style of interaction and development philosophy. All information is common to the same information domain. Common files are always used. A package will not pass design review or verification if it creates its own file when an existing file would serve. To the user and site manager, this means that duplicate information never needs to be reentered. For example, once the temporary address is entered into the patient data base by the Medical Administration Service (MAS) personnel, all packages immediately have access to that data with no additional programming required by any software package. Practically, this means that the pharmacist will immediately know that the patient is at a different location than the home address, which will result in elimination of useless mailing of medications to a veteran who will be away from home for the next several weeks. Since all files and data reside in an environment under a common data base, retrieval of data from this integrated data base is much easier than retrieval of similar data from an environment which requires torturous routing through interfaces between different data environments. Unlike other systems, DHCP design started from a concept of a technically totally integrated system; therefore, integration is built in and not tacked on as an afterthought.

True integration is built in from the initial design stages and carried on through every step of system design. Apparent integration can exist in a system that has very little real technical integration. In such systems, the apparent integration is achieved through substantial and continuous software programming efforts to develop and maintain an interface among application modules.

DHCP is an integrated system, as GAO has recognized. The IHS systems are not integrated in the true sense but have elaborate interfaces among applications and, in some cases, among totally different hardware systems. Maintenance of an interfaced system is much more difficult and costly than maintenance of an integrated system because every time there is a change in one application, all its software interfaces with other applications must be changed.

2.

With respect to the scope of the program, the report states that Core plus 22 Enhanced and 23 Comprehensive modules comprise DHCP. This is no longer correct. It is Agency and Office of Management and Budget (OMB) policy that DHCP is composed of only those applications which have been shown to have net benefit over their life cycle (10 years). These applications are Core plus Radiology, Dietetics, Records Tracking, Integrated Funds Control/Control Point Activity/Accounting and Procurement (IFCAP), Surgery, Decentralized Medical Management System (DMMS), Nursing, and Mental Health. Only as other applications are considered to be cost-justified and approved by OMB will they be added to DHCP.

CHAPTER 2: OPERATIONAL DHCP SATISFIES USERS BUT HAS SOME SHORTCOMINGS

Chapter 2 discusses the software development process, including verification and testing, and expresses concern about the early release of software and failure to comply with federal guidelines. The chapter goes on to discuss internal software controls, hardware and software tracking, and security. The well researched data presented in the report identify a number of weaknesses in the DHCP program when it was first installed in 1983. Our response describes the steps that are already in process or planned to correct these deficiencies. GAO recognizes many of these in its report. In most cases, policy documents addressing these issues have been promulgated or are in the concurrence process. The following discussion highlights the issues and provides responses which detail the corrective action we are taking to resolve problems and supports the VA's position where it differs from GAO.

DHCP Management

Now on pp 18-23.

Now on pp. 25-26.

GAO has noted that among the factors contributing to problems with DHCP system development efforts are inadequate central management control (pages 24-31) and the absence of a methodology to track software and hardware problems (pages 34-35).

DHCP was designed to support the field elements of the Department of Medicine and Surgery (DM&S). The first step was to provide this support for the critical areas of MAS, Pharmacy, and Laboratory by procuring and deploying equipment and developing and deploying software.

Under the decentralization concept, the various responsibilities for planning, direction, and control rested with different entities at different levels of the DM&S organization. A major focus of the program was the deployment of equipment and implementation of systems at the VA Medical Centers (VAMC's). These activities required intensive coordination at the regional level. In recognition of this, the line authority over the Information Systems Centers (ISC's) was transferred from Medical Information Resources Management Office (MIRMO) to the regional directors in a Chief Medical Director Memorandum dated July 1983. This gave a great amount of responsibility for the program to each region and was effective in many areas: system implementation, such as refinement of regional priorities for the implementation of DHCP modules on a nationwide basis; implementation of a system for facility automated data processing (ADP) planning; and preparation and establishment of regional ADP support priorities.

3.

At the end of this intensive system implementation phase, such factors as system refinement, fine-tuning, module interaction, software integrity, and standardization of day-to-day operations became much more important. To strengthen national coordination and direction in order to satisfy these needs, in a DM&S reorganization on February 24, 1987, the Administrator approved the DM&S proposal that the regional ISC's report directly to MIRMO. The realignment of the ISC's under the line authority of MIRMO will serve to strengthen the project management and accountability on issues of national priority while retaining in the regions and the medical centers the necessary degree of control over matters more appropriately addressed at those levels.

DHCP Problem Tracking

We do not understand GAO's stated concerns over problem tracking or their assertion that software and hardware problems should be tracked and corrected before additional hardware is acquired. Tracking and correcting problems is an ongoing process in any dynamic program like DHCP. VA has multiple mechanisms for dealing with them.

Computer hardware problems are tracked jointly by the site manager, local vendor representatives, and the respective ISC. There is also an established national maintenance contract to support hardware problems. The contracting officer and the appropriate vendors are responsible for tracking and resolving these hardware problems. Each ISC is responsible for tracking the frequency of hardware/software problems for stations under their jurisdiction. Exception situations are identified by the ISC and handled by the contracting officer's technical representative (COTR). For incidents of a repetitive nature, the VA uses its nationwide electronic mail system to disperse information pertaining to problems and suggested resolutions for matters of national significance.

With respect to operating systems problems, the VA has a nationwide contract with the Digital Equipment Corporation (DEC), the major DHCP equipment vendor, to provide 24-hour, 7-days-a-week phone consultation on operating system matters. The Agency has requested similar support from the vendor (Intersystems) supporting the small VA hospitals and is waiting for a proposal. Unresolved problems are referred to the COTR for resolution.

Application software problems, resolutions, and frequency of occurrence are tracked for use at various levels of the management structure. One methodology which is being considered for implementation across all packages was developed by the Laboratory users. A format called the E3R (Electronic Error Enhancement Report) allows users nationwide to report system deficiencies, system errors, and desired enhancements in a standardized format via the electronic mail system. These reports are reviewed by each VAMC Laboratory System Coordinator, the developing ISC, and MIRMO. The reports are then evaluated, solutions determined, and corrections transmitted to the field via electronic mail or prioritized for input to future release of application packages.

The VA has developed a national patch system where all centralized software fixes are posted. All sites have access to this system through the nationwide electronic mail system. In addition, there are regional support endeavors, through the ISC's, where a support group staffed by applications specialists is available to provide assistance on software problems.

4.

A system to track the installation of both hardware and software has been implemented. All VAMC's report status quarterly to the Washington ISC that produced the first report in April 1987. Work has also begun on a DHCP project tracking system for MIRMO oversight and management of all DM&S information resources. A contractor is preparing specifications for a tracking system that will include, but not be limited to, tracking national software development by the ISC's and program management issues.

DHCP Policies and Procedures

Now on pp. 23-24

The report indicates that VA had only an informal software development policy addressing documentation, verification, testing, and approval procedures. As a result, initial software contained errors and failed to follow federal guidelines (OMB Circular A-130, FIPS 31, 38, 64, 102, 105) (Chapter 2, pages 31-33). That is essentially correct through December 1986 when formal verification policy was issued.

From 1983 to 1986, our number one priority was to establish a baseline of Core software at the medical centers as quickly as possible to help the facilities keep pace with their expanding workload. This goal was realized, but at the expense of thorough documentation and rigorous quality control. Recognizing this, DM&S has implemented improvements in the last 12 months. No new package is being released without a full complement of user and technical documentation. User and technical documentation for Initial/Full Core products will be complete and up-to-date by the end of the calendar year. Documentation standards are being put into place and responsibility for assuring conformance to those standards is being centralized at one location. We are also investigating the development of on-line documentation through the use of "help" screens. This would provide live documentation support to the user and not interrupt use of the terminal. Software quality control has also been strengthened. Each package is now verified by both the ISC responsible for development and by another ISC prior to MIRMO release for distribution to the medical centers. Additional positions were given to each ISC by MIRMO to hire verifiers and documenters. The alpha/beta testing process has also been expanded to assure that the modules are tested both in medical centers using DEC operating systems and those using Intersystems Standard MUMPS (ISM). (MUMPS is the language used in DHCP.) After formal software release, the ISC's typically distribute an application to selected sites prior to general distribution; this has proven to provide a further level of quality control. The result has been much higher quality packages arriving at the medical centers.

DM&S has taken several other steps to improve compliance with federal guidelines:

-- Verification guidelines that ensure "required administrative, technical and physical safeguards are operationally adequate" (OMB Circular A-130) have been developed and were issued December 9, 1986.

-- Software documentation guidelines have been developed and were issued May 15, 1987.

-- DM&S circulars addressing security policies are being written to replace interim issues.

5.

Now on pp 23-24

In order to ensure that medical center development and testing is in compliance with applicable federal guidelines (page 33), the Agency issued DM&S Circular 10-85-93. This document restricts local modifications to national software packages and outlines the methodology (such as name spacing conventions and requisite standards) which must be adhered to in making such modifications. Using VA File Manager, local facilities can add site-specific items without affecting the integrity of the data base or the standard nationally developed software.

The Federal Information Processing Standards (FIPS) are guidelines geared more to the development of traditional large centrally operated computer systems and their commonly used languages. They do not adequately address the prototyping methodology inherent in the DHCP. But now that MUMPS has become a FIPS standard, we expect that the other FIPS guidelines will be modified to take account of MUMPS' inherent strengths and differences.

DHCP Data Integrity

Now on p. 26.
Now on pp. 27, 29

The report states that VA software controls do not prevent incorrect or unauthorized data entry (page 33), the accidental creation of multiple patient records (page 36), or the alteration of patient eligibility data (page 40).

Regarding the statement that the software does not adequately prevent incorrect or unauthorized data entry, it should be noted that the DHCP system software environment includes multiple mechanisms to ensure that only correct data are added to files and that unauthorized entry is prohibited. The DHCP software includes the following features:

-- A security sign-on module, that requires each user to enter an "access" and a "verify" code to gain access to the system, is incorporated.

-- Each user is given a selective menu of functions and files that further restricts which data they may see and whether they can add or change data.

-- The user must have proper file security codes to interact with the VA File Manager Files.

-- The user must be given the authorized security code (an electronic password) in order to complete designated activities.

-- Each data element entered into any file is validated by an "input transform" before it enters the data base.

VA believes that these DHCP software controls are more than adequate to prevent unauthorized data entry.

6.

The DHCP systems have several features to prevent duplicate data entry. They:

-- do not allow for the creation of duplicate social security numbers (SSN's) for different patients,

-- do not allow the assignment of differing SSN's to the same patient, and

-- require that data entry personnel certify that a new patient is to be added to the data base when the system does not find a match for a patient who has been entered.

With respect to the GAO finding that the software does not prevent the accidental creation of multiple patient records, we have already corrected some of the conditions cited. Specifically, the software now screens for blank spaces between the first and last names to prevent this from being recognized as two patients. We have found, as the GAO report corroborated, that under some conditions it is still possible to create duplicate patient records. We are actively working on technical methods to ensure that the data entered are accurate. We will also develop data base validation programs in each medical center to have staff review existing data bases, identify potential duplicate patients, and merge duplicate records. This two-pronged effort should minimize a problem that we agree warrants our immediate attention. A meeting of developers and users was held in early May 1987 to resolve this issue and assign development tasks necessary to correct the situation. We expect that an automated patient merge routine will be available in late 1987. In the interim, the next version of the Admissions/Discharge/Transfer (ADT) software, currently scheduled for release in May/June 1987, will contain a revised patient look-up algorithm that checks a number of key indicators to identify possible duplicate entries before adding a new patient record. It is important to note, however, that no amount of automated software checking and validation will eliminate the requirement for staff data validation review and a quality assurance program for systems of records, automated or manual.

Another problem cited by GAO, the alteration of patient eligibility data, was also identified by the Special Interest User Groups (SIUG's), users, and others as a problem. The DHCP software, while providing a multitude of mechanisms to enforce the entry of correct data by authorized individuals, had a flaw. Anyone who was authorized to change data could change eligibility data. A verified eligibility status could be altered to become an inappropriate one inadvertently or intentionally without any change in the notation that the status was verified.

This situation was corrected with the release of version 3.5 of the ADT package in April 1987. The software will now allow only a holder of a specific password to verify patient eligibility. Once eligibility has been verified, it is not possible to change the eligibility status unless one is also authorized to verify eligibility by virtue of possessing the password. In addition, when the eligibility status is updated after initial verification of eligibility, an audit trail is created identifying the authorized user responsible for the change.

7.

DHCP Security

GAO takes the position that VA's internal controls are not adequate to prevent compromise of patient data or the interruption of computer support. We believe that we have made substantial progress in this area and are continuing to strengthen this aspect of the program.

The first DM&S ADP Security Policy and Guidelines were issued in August 1985. Since the issuance of those guidelines, the national program has been reexamined and the circular is being revised. When it is reissued in October 1987, it will have, in addition to ADP security policy that applies to all DM&S offices and facilities, three sets of guidelines: for VAMC's, ISC's, and VA Central Office. These guidelines will serve as the basis upon which each DM&S entity is to develop ADP security procedures specific to their organization and physical plant.

As discussed in the report, DM&S ADP Security Program staffing has been less than adequate. To provide the necessary staff, on February 19, 1987, the DM&S Director for Operations approved additional positions to be located at the Martinsburg VAMC as an adjunct staff of the MIRMO ADP Security Program. The primary responsibility of this adjunct staff will be to monitor compliance with DM&S policy and guidelines. Periodic assessment by the DM&S ADP Security Staff will supplement the annual self-assessment required of each site. An assessment tool will be part of the guidelines. Of course, the Inspector General will continue to audit ADP security as an element of recurring site visits.

The GAO report indicates that under the Federal Managers' Financial Integrity Act, DM&S' ADP security is a material weakness. We recognize our responsibility to comply with the Act, and the DM&S internal control program continues to identify ADP security as a high risk area. Planned corrective actions are included in the circular to be issued in October.

Now on pp 33-34

GAO also expressed concern that releasing software under the Freedom of Information Act (FOIA) increased the risk of unauthorized access (page 47). This issue was also raised by the VA Inspector General. In June of 1986, the Chief Medical Director requested the VA General Counsel to consider the appropriateness of discretionary withholding from FOIA disclosure any DHCP software that controls access to the system or that ensures the integrity of applications processing and internal controls. The General Counsel's response indicated that existing FOIA exemptions permit the discretionary withholding DM&S requested. A circular now in the concurrence process will implement this discretionary authority. We have already implemented the practice of discretionary disclosure in advance of the circular release. The latest version of the "Kernel" application, which controls access to DHCP and contains the DHCP security algorithms, is being released in two versions. Kernel software and documentation, containing sensitive data, are distributed only within DM&S. The "public domain" version of software and documentation is released with this sensitive code deleted.

8.

Now on p 31.

The GAO report also discusses the lack of disaster recovery plans and how this may result in difficulties and delays in restoring computer operations following damage or destruction (page 44).

DM&S officials have been aware of this problem from the inception of the hospital automation program. After performing a cost-benefit analysis and exploring alternative plans for recovery (e.g., procurement of a reserved spare computer system), MIRMO procured, for all DHCP sites except smaller facilities (Class V), complete coverage by a major vendor's contingency maintenance program. Under this extensive disaster recovery plan that was effective October 1986, appropriate DHCP system components--or the whole system if necessary--are replaced within 2 weeks in the event of partial or total destruction of a medical center's computing capacity. We are in the middle of contract negotiations to provide contingency maintenance for the Class V hospitals.

Now on p 32

In this chapter (pages 44-45) GAO states "In December 1986, VA drafted an ADP circular that requires risk analyses and contingency plans at each ADP location. This draft circular specifies when risk analyses and contingency plans are to be conducted at Information Systems Centers and provides an audit guide for the Inspector General's use in ensuring that the Information Systems Centers comply with the policy." This statement is in error. The Office of Inspector General is not responsible for administering the Agency ADP security program. The Inspector General's role and responsibility are those of review and oversight.

CHAPTER 3: DHCP EXPANSION PLANNED WITHOUT INFORMATION NECESSARY FOR INFORMED DECISIONS

The discussion in Chapter 3 is critical of VA's planned expansion for hardware, software, and telecommunications. The lack of an adequate cost-benefit analysis is pointed to as the major reason. The report is also critical of the Agency's monitoring of system utilization and capacity planning, lack of alternative configuration assessment, and central management's role in the development of the order entry feature. The following discussion describes the VA's plans for improving utilization and capacity management and discusses the cost-benefit analysis of the top priority applications. The enhanced role of central management is also discussed as it relates to implementation of Order Entry options.

Estimating DHCP Hardware Needs

Now on p 36

GAO claims that DHCP expansion plans include substantial amounts of software, hardware, and telecommunications (page 51). Although the VA ADP plan lists 22 Enhanced and 23 Comprehensive applications, they are only potential areas for future automation. It is Agency and OMB policy that DHCP be limited to Core and the eight priority enhanced DHCP applications (Radiology, Dietetics,

9.

Medical Records Tracking, IFCAP, Surgery, Nursing, Mental Health, and DMMS) which have been cost-justified and approved. The fiscal year (FY) 1988 budget request submitted in January 1987 makes this clear. Funding to buy equipment for these applications is needed in FY 1987-FY 1989, not through FY 1996.

Now Appendix II and III, pp. 66-68

We would also like to clarify information contained in Appendix II "Development Status of VA's DHCP Enhanced and Comprehensive Modules" (pages 88-89). Implementation status for the first six items on the chart is accurate; however, application #7, Mental Health, and application #8, Nursing, are scheduled for implementation in FY 1989, not FY 1988. No other modules listed on the chart are currently approved for implementation. Their inclusion in DHCP will be based on the outcome of future cost-benefit studies.

The Agency has developed a model for estimating equipment support, based on various clinical and administrative parameters. This model includes data to calculate the capacity required for Core and Enhanced DHCP. The application of this model yields equipment requirements for DHCP health care facilities in terms of through-put units, disk capacity, and terminals. Office of Inspector General staff reviewed the model and found it to be reasonable.

GAO feels that VA has selected a decentralized hardware configuration with on-site computers without considering the cost-effectiveness of other alternatives, such as regionalized computer centers or a combination of the two approaches. They also state that Agencies are required to perform a comparative cost analysis (FIRMR: Federal Information Resources Management Regulation) and a requirements analysis (FIRMR 201-20.003) before proceeding with system acquisition.

The VA reviewed the FIRMR's cited by GAO and met with General Services Administration (GSA) officials. It was determined that the VA is in full compliance with both of these regulations. This is evidenced by the Requirements Analysis and Comparative Cost Analysis that were submitted to GSA to obtain the Delegation of Procurement Authority they granted in March 1987, based on the VA's compliance with appropriate GSA procurement regulations.

FIRMR 201-30.009 provides a list of alternatives to be considered by agencies, and each was thoroughly addressed by the VA. The issue of regionalization was not among the alternatives contained in the FIRMR. The VA did not readdress this issue because it was implicitly evaluated and determined not to be cost-effective for providing computer support to VA medical centers.

The Agency rejected a regionalized systems approach because it compromises critical aspects of the DMIS information management program. Computers are a critical resource of hospital managers and they should be able to control and

10.

be responsible for them as for any other resource in a hospital. Furthermore, regionalized systems supporting many medical centers for their local transactions from a remote site would make the DHCP program more costly, inefficient, and nonresponsive to users. For example:

-- Due to the highly interactive multitransactional use of DHCP applications, such as MAS and laboratory, required for effective operational support of VAMC functions, any regionalization or centralization scenario will cause national telecommunications costs to soar.

-- Regional or central computer installations that serve multiple VAMC's are necessarily more complex than single hospital systems and pose significantly increased management and technical problems.

-- Consequences of systems failure are greater because several VAMC's would lose their processing capabilities at the same time.

-- On-site help is not available to solve hardware or software problems if a user at one of the VAMC's (e.g., a physician, pharmacist, or nurse) encounters a problem.

-- Remote systems become increasingly bureaucratic and unresponsive to users. This was a problem in the past and was one of the major reasons for implementing a decentralized system to support local hospital operations.

After congressional review of the regionalized VA Computerized Medical Information Support System (COMISS) in 1982, its termination was ordered. We do not intend to revisit the issue of regionalization of local processing. We do have plans to continue to regionalize or centralize the collection of certain aggregate data and selective patient information on a national basis, i.e., the Patient Treatment File, for management information and reporting purposes.

GAO states that VA has not regularly monitored the use and available capacity of DHCP computers. We do not agree with this observation. Regular monitoring of computer utilization and available capacity is an integral part of good site management. The site manager at each DM&S facility has access to vendor-supplied software routines which gather information on how system resources are being used. Moreover, the ISC's have developed tuning guidelines to assist the site managers in configuring their systems to get maximum efficiency. A capacity tuning group under the Washington ISC is developing a System Tuning Seminar to be included as part of the continuing training effort in DHCP. In addition, the Agency has just recently signed an interagency agreement with GSA's Federal Computer Performance Evaluation and Simulation Center (FEDSIM) to provide technical support to DM&S to configure and fine tune its systems more effectively. Other benefits derived from this contract include the development of additional performance tools by a third party vendor, a handbook and training course outline which provides procedures, tools and reporting requirements; and means for analyzing improvements in capacity planning. In addition, the systems support staff of each ISC is always available to assist sites in utilizing all available capacity management tools.

11.

DHCP Order Entry/Results Reporting

Now on p. 48.

The report is critical of VA Central Office management's ability to obtain a consensus on the DHCP order/entry procedures (page 65). As discussed in the response to Chapter 2, the recent reorganization within DM&S gave the Director of MIRMO direct line authority over the Information Systems Centers, thereby providing the management office with additional centralized management authority. Completion/development of the Order Entry/Results Reporting Options (OE/RR) has been accelerated to number one priority of the ISC's by the Director of MIRMO. In May 1987, developers and users of several affected packages met to resolve any outstanding issues and agreed to necessary software changes.

The OE/RR feature is a system of patient-oriented utilities and standards that refines current capabilities to place orders for all modules from within any module. More important, the results reporting function will allow the user to view all test data on a patient displayed on a single screen. It also provides additional capabilities which include: 1) uniform displays of order status; 2) verification of orders prior to activation within the governing module (e.g., orders may be placed by provider, entered by clerk, reviewed and approved by nurse); 3) the ability to identify the patient before, rather than after, the department/service is selected; 4) linking components of complex orders involving multiple services; and 5) providing a technical framework for installing decision-support system logic.

The first version of OE/RR will contain the first three of these capabilities and is being tested. It will be available this summer for beta testing with several applications.

DHCP System Life Cycle Costs

GAO has criticized the VA for not including all possible costs in its DHCP systems life cycle estimate. To respond to this criticism, we have prepared a new set of estimates which take account of the GAO criticisms. Major changes include the following:

-- We use a 10-year life cycle (1987-1996) for all of DHCP (Core plus the eight approved applications in Enhanced DHCP). This is consistent with the life cycle used in the Booz-Allen and Hamilton study of DHCP and IHS. All recurring and nonrecurring costs for those years are included.

-- There is an increase in VAMC staffing, sufficient to bring all sites up to the recently developed DHCP staffing guidelines by 1992.

12.

-- Telecommunciations costs are included. Our estimate of $14,185,000 is significantly lower than the GAO estimate. DHCP is a system for local VAMC operations, and only a small portion of total DM&S telecommunications costs (largely for Hospital Inquiry (HINQ) and DMMS) are appropriately charged to DHCP. Costs of communicating to central systems are all allocated to those systems. We want to state that the estimate of telecommunications costs is a much rougher estimate than any of the other line items. We are currently pressing for a more accurate accounting system for telecommunications. Nonetheless, it is certain that only a small portion of total DM&S telecommunications costs are appropriately charged to DHCP.

-- Utility costs are now included, although our estimates are higher than GAO's.

-- Applications coordinators and time that SIUG personnel spend on DHCP are included.

-- Site preparation costs are based on actual requests from medical centers.

Additionally, we are now using a fringe benefit rate of 16 percent for 1987 and 20 percent for subsequent years. This is the same fringe benefit rate that is used for internal budgeting.

With these adjustments, the total 10-year life cycle cost is $878,215,000. If a fringe benefit rate of 34.35 percent were used (reflecting the Government's full share of retirement costs, not just VA costs), the life cycle cost would be $924,880,000.

Life cycle costs by year and line item are shown in the following table. It should be noted that these costs are under continual review, and are subject to adjustments to reflect actual expenditures, new policy guidelines (e.g., OMB passbacks and congressional action), and changes in fringe benefits.

See following page for the Summary of DHCP Life Cycle Costs.

SUMMARY OF DHCP
LIFE CYCLE COSTS
($000's)

COST COMPONENT	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	TOTAL
VACO FTEE	16	18	20	20	20	20	20	20	20	20	0
VACO PAY & BENEFITS	521	586	651	651	651	651	651	651	651	651	6,315
VACO FRINGE BENEFITS	83	117	130	130	130	130	130	130	130	130	1,242
VAMC FTEE	395	467	549	635	716	812	852	852	852	852	0
VAMC PAY & BENEFITS	9,583	11,330	13,459	15,796	17,996	20,605	21,692	21,692	21,692	21,692	175,537
VAMC FRINGE BENEFITS	1,533	2,266	2,692	3,159	3,599	4,121	4,338	4,338	4,338	4,338	34,724
ISC FTEE	236	261	261	261	261	261	260	260	259	259	0
ISC PAY & BENEFITS	6,986	7,769	7,769	7,769	7,769	7,769	7,752	7,736	7,720	7,703	76,742
ISC FRINGE BENEFITS	1,118	1,554	1,554	1,554	1,554	1,554	1,550	1,547	1,544	1,541	15,069
SIUG FTEE	10	10	10	10	10	10	10	10	10	10	0
SIUG PAY & BENEFITS	326	326	326	326	326	326	326	326	326	326	3,260
SIUG FRINGE BENEFITS	52	65	65	65	65	65	65	65	65	65	639
APP COOR FTEE	203	204	291	280	225	185	178	178	178	178	0
APP COOR PAY & BENEFITS	5,510	5,539	7,889	7,609	6,105	5,030	4,816	4,816	4,816	4,816	56,946
APP COOR FRINGE BENEFITS	882	1,108	1,578	1,522	1,221	1,006	963	963	963	963	11,169
PROG TRAVEL	943	1,088	1,210	1,338	1,459	1,603	1,662	1,661	1,660	1,660	14,284
TRAINING TRAVEL	49	41	78	104	92	84	69	69	69	69	724
SIUG TRAVEL	26	26	26	26	26	26	26	26	26	26	260
SOFTWARE MAINT	1,090	1,090	1,547	1,807	2,185	2,185	2,101	2,078	2,127	2,163	18,373
HARDWARE MAINT	9,836	9,836	14,038	16,430	19,910	19,910	19,148	18,184	17,655	17,451	162,398
MISC CONTRACTS	1,286	1,344	1,344	1,708	1,708	1,708	1,705	1,701	1,697	1,694	15,895
FED TRNG	122	102	194	257	228	208	170	170	170	170	1,791
COMMERCIAL TRNG	168	268	268	268	268	268	268	268	268	268	2,580
RECORDING MEDIA	372	213	1,139	833	1,126	435	435	435	435	435	5,858
OPERATING SUPPLIES	3,115	3,115	4,459	5,224	6,337	6,337	6,337	6,337	6,337	6,337	53,935
TELECOM	697	896	1,207	1,485	1,650	1,650	1,650	1,650	1,650	1,650	14,185
UTILITIES	1,040	1,336	1,801	2,215	2,460	2,460	2,460	2,460	2,460	2,460	21,152
ADDL EQUIP	35,018	19,932	29,000	0	0	0	19,047	24,110	13,220	5,098	145,425
REPLACEMT EQUIP	528	578	819	959	1,162	1,162	1,117	1,106	1,131	1,150	9,712
SITE PREP	15,000	15,000	0	0	0	0	0	0	0	0	30,000
TOTAL	95,884	85,525	93,243	71,235	78,027	79,293	98,479	102,520	91,151	82,857	878,215
CUMULATIVE	95,884	181,409	274,652	345,887	423,915	503,208	601,687	704,207	795,358	878,215	

* Federal personnel costs reflect an assumed 18 percent fringe benefit rate in FY1987 and 20 percent in FY1988-96

14.

Cost-Benefit Analysis

The report is critical of the cost-benefit analysis of Enhanced DHCP that was done in 1986. Many of the points raised by GAO are valid. On the basis of new life cycle costs, we asked Price Waterhouse to update and revise their analysis using detailed information on the functionality of the enhanced DHCP applications. The new analysis shows a rate of return of 9 percent. This is equivalent to a present value of net savings of -$5,470,000, using a 10 percent discount rate.

At our request, Price Waterhouse did a number of sensitivity analyses. The most important of these replaces the fringe benefit rate of 34.35 percent, which was used in the base analysis, with a fringe benefit rate of 16 percent in FY 1987 and 20 percent in subsequent years. The rate used in the base analysis (34.35) is an estimate of the full cost to the Government of retirement and other fringe benefits. The lower rate, which is the one used by VA for budgeting, reflects only the cost to the Agency. At the lower rate, the rate of return is 6.4 percent; the present value of net savings over the 10-year life cycle, using a 10 percent discount rate, is -$18,191,000.

The analysis is conservative in that no attempt was made to place a dollar value on qualitative benefits. The analysis

-- uses revised life cycle costs that have been corrected to rectify omissions identified by GAO and updated to reflect policy changes (e.g., the new fringe benefit rates brought about by changes in the federal retirement system) and new information.

-- covers eight rather than nine applications. Two changes have been made: fiscal and supply have been combined as IFCAP, and the Decentralized Medical Management System has replaced personnel. This latter decision was made during the formulation of the FY 1988 budget because of the urgency of obtaining better management information to improve productivity and utilize resources more effectively. (Most pressing personnel needs will be met by the redesign of the Agencywide Personnel Accounting Integrated Data (PAID) system.)

-- revises benefits to take account of changes in fringe benefits (for personnel savings) and changes in functionality. IFCAP benefits were recalculated by the users who now are more familiar with the package and have greater confidence in its ability to produce savings.

-- uses revised estimates for anticipated salary increases.

-- uses a new implementation schedule reflecting the current budget and procurement schedule.

-- follows the guidelines of FIPS 64, insofar as that is feasible and appropriate.

IS.

In the original cost-benefit analysis and in the current one, the comparison is between continuing to automate through DHCP and maintaining a manual system. We believe that this satisfies the intent of FIPS 64. We did not consider a regional configuration because the purpose was to determine whether to extend the existing decentralized system.

It is not necessary to compare DHCP with a commercial system as part of the cost-benefit analysis because we commissioned a major cost-effectiveness study (the Booz-Allen and Hamilton study) comparing a commercial systems approach (IHS) with DHCP. This study showed that a comparable system (one that performed the same functions) would cost twice as much under IHS as under DHCP. At our request, Booz-Allen has reestimated the life cycle costs of automating under the IHS approach using the methodology recommended by GAO. They still find that IHS is significantly more costly than DHCP--the percentage difference in costs is in the range of 73-81 percent, depending on the fringe benefit assumptions that are used. Furthermore, they have now modified their effectiveness findings; they state that the increased staff resources we plan to devote to DHCP "can be expected to result in significant improvements in future DHCP support services and management support." (See Enclosure 3.)

Personnel savings were estimated by program personnel familiar with both the service's manual operations and the proposed automation. The operations to be automated and their costs were identified, and the impact of automation estimated.

We believe that the methodology used here--a prospective cost-benefit analysis based on a clear understanding of the functionality of the proposed applications and the operations to be automated, and using program experts to estimate the impact on operations--was preferable to a methodology requiring new site-specific data collection. However, both costs and benefits of proposed applications are under continuing review and analysis. Just as we continue to refine our cost estimates to reflect actual expenditures and changes in policy, we also continue to monitor the benefits as software is more fully developed and tested, and we will continue to conduct postimplementation evaluations on all applications. The revised cost-benefit analysis appears as Enclosure 4.

Not included in Report.

CHAPTER 4: COMMERCIAL SYSTEMS' TEST NOT APPROPRIATELY STRUCTURED TO COMPARE COSTS AND BENEFITS

This chapter correctly points out that the DHCP and IHS programs were originally conceived with different purposes and scope, making comparison difficult but not impossible. DHCP is an ongoing VA-wide operational program, while IHS is a test program undertaken at three sites to test three separate vendors' products. However, comparison is possible because the two approaches are functionally similar, and by virtue of being ADP systems, have many of the same cost factors and potential benefits.

lo.

Booz-Allen and Hamilton was able to normalize key elements of each approach and to compare them on cost and effectiveness. The net result was that for the same set of functions (Core plus the eight additional functions designated by VA top management as highest priority) and the same 10-year life cycle (FY 87 to FY 96), DHCP was found to be significantly cheaper. In that study, the costs of both systems for a 10-year life cycle were $777 million for DHCP versus $1.5 billion for IHS. The study also found that the cheaper DHCP system was more acceptable to end users than IHS. These dual findings reaffirmed for DM&S that it should proceed with plans for additional equipment to expand DHCP to provide more functions and serve more users. We have no specific plans to phase out IHS at the three medical centers. Vendors will be expected to continue operations of these systems throughout FY 88.

Since publication of the Booz-Allen study this February, we revised the DHCP cost estimates to include additional factors (the most significant of which is application coordinator time) and asked Booz-Allen to do the same for its IHS projections. Revised estimates for both IHS and DHCP are higher, but IHS remains significantly more expensive.

Differences Between the Two Approaches

The purpose of DHCP is to provide comprehensive information systems support to 169 VAMC's and satellite facilities (225 medical care facilities in all) and management support to DM&S. It is a fully operational DM&S-wide program, not a test. Since delivery of the first DHCP equipment in March 1984, we have installed DHCP equipment and software in support of 225 facilities of widely varying sizes and complexity. In the process we have hired and trained an ADP support infrastructure at the local, regional, and central office level. Under centralized procurements we have installed 480 central processing units (CPU's), 19,000 cathode ray tubes (CRT's), and 9,000 printers. The software that we release nationally must be generic while at the same time adaptable to the unique requirements of each VAMC. DHCP clearly is a very large scale effort that has required and received commitment and support from all levels of management.

In contrast to DHCP, the IHS project was conceived in 1984 as a test of the applicability of off-the-shelf software at VA medical centers and the ability of commercial vendors to customize their software to meet the specialized needs of VA users. It was limited to three facilities and was not intended as a vehicle for comparing commercial systems to DHCP. The vendors were given latitude in what applications they offered beyond the mandatory ones, in system design, equipment configuration, and implementation strategies to allow them to maximize the effectiveness of their individual products. At the same time they were required to meet central system reporting requirements by supplying data in the formats and according to the definitions required by those systems.

17.

IHS was conceived as an experiment whereby three different vendors would install their hospital information systems software at three discrete medical centers of differing sizes and complexity: small (Big Spring), medium (Saginaw), and large (Philadelphia). The three test facilities that were selected do, in fact, represent a range of size and complexity. A number of different factors in addition to the number of operating beds contribute to the VA's complexity ratings of facilities and to the model used for projecting DHCP equipment requirements. The complexity ratings are used by the VA as an aid for relating top management responsibilities to compensation, such as salaries, awards, job classification, and assignments. Under both measures Philadelphia ranks among the largest hospitals. It is in the top 10 percent nationwide in overall complexity and in the top 20 percent in the DHCP equipment sizing model.

The IHS contracts were not intended to be expandable to all facilities. As noted in the GAO report, contracts with nationwide scope would have to deal with the potential economies of scale. They would also have to deal with the management implications inherent in nationwide programs that are quite different from the vendor/customer relationships experienced in the IHS single site implementations. From the widely different estimates vendors provided the GAO, as well as the caveats placed on them, it appears that the vendors themselves are not certain what nationwide implementation and operations would involve.

The vendors' unproven assertion that they could provide computer services nationally at less cost to VA if they used large computer centers serving many hospitals is not relevant. Use of regional computers for local operations is not acceptable to the VA. Moreover, in the unlikely event that local performance and response requirements could be met without driving telecommunications costs to unacceptable levels, such regionalization could be achieved in-house through DHCP. It is, therefore, not useful in any discussion of DHCP versus IHS.

Now on pp. 51-52

The IHS vendor contracts limit each vendor to installing their system in only one of three sizes of medical centers, as noted on page 71 of the GAO report. This contract limitation was based on the assumption that if a commercial system package was successful at one particular medical center, it had the potential for being equally successful at a second facility of comparable size and complexity. The same assumption did not extend to medical centers that vary in size and scope from the contracted facility. In order to install one IHS vendor system at all VA medical centers it would be necessary to obtain a new delegation of procurement authority which would be in the form of either a competitive procurement or a sole-source contract. Given the number of qualified vendors in the marketplace, the latter would be difficult to justify.

18.

The Basis for Comparability

Despite differences between approaches, the Booz-Allen study was able to normalize key cost and effectiveness elements and established a single 10-year life cycle period. The comparison made in this study used the VA's requirements (Core plus the eight additional modules selected by VA management and approved by OMB) as a baseline for comparing cost effectiveness over a period extending 10 years into the future. Booz-Allen identified 17 generic functions. Of these, the current IHS contracts address 14, which suggests that the two systems' features are largely comparable. Booz-Allen further assumed that the missing functions were available in the marketplace and included them in life cycle cost projections. They then developed scenarios explaining how requirements would be met over a 10-year life cycle beginning in FY 87, broke these scenarios into resource components, and costed each component for both an in-house and a commercial acquisition approach. They assumed a single nationwide contract for IHS, consulted with the three vendors and others, and adjusted the original contract prices to account for economies of scale.

We believe that the Booz-Allen study statistically adjusted for any design differences between the DHCP and IHS approaches and provides a valid cost comparison.

BOOZ ALLEN & HAMILTON INC.

4330 EAST WEST HIGHWAY • BETHESDA MARYLAND 20814-4455 • TELEPHONE (301) 951-2200 • TELEX II 710 924 0552

May 29, 1987

David Van Hooser, Director
Veterans Administration
Medical Information Resource
  Management Office
Room 664
810 Vermont Avenue
Washington, DC 20420

Dear Mr. Van Hooser:

As requested, we have reviewed your revised DHCP life cycle cost estimate. Our understanding is that the revised estimate incorporates adjustments we made to the original DHCP life cycle cost estimates and comments made by the GAO in their recent study of DHCP.

Our review of the estimate focused on two areas. It was conducted to determine:

- The reasonableness of additional changes you have made to the DHCP life cycle cost estimate we developed in the DHCP/IHS Comparability Study
- The impact of those changed assumptions on study findings.

Based on data available to us, we believe the changes that have been made are reasonable. For the most part, the changes reflect more refined cost component information and changed future assumptions. The changes result in increases in both the DHCP and IHS life cycle cost estimates. Those changes do not change our cost findings; however, we believe they could result in changes to our comparative effectiveness findings. These results are described in more detail below.

CHANGES IN DHCP LIFE CYCLE COST ESTIMATE

From our review of your revised estimate we have identified four significant differences from the DHCP life cycle cost estimate we developed for our study:

- Additional ISC and VAMC FTEE--The revised estimate assumes more FTEEs in the ISCs and VAMCs than was assumed for our estimate. We have no problems with this changed assumption since we believe more

support at those levels will address problems we anticipated in future DHCP effectiveness. (Note the potential impact on our effectiveness findings in the next section.)

- Application Coordinators--The revised estimate includes pay and benefits costs for application coordinators, a cost that was not included in our estimate. We believe that it is reasonable to include this cost in the life cycle. We do not have data to determine whether the amount included is accurate; however, it appears to be close to the amount estimated by the GAO.

- Changes attributeable to more refined cost information--We note changes in training, installation, telecommunications, utilities, and equipment costs. From back-up information provided with the estaimate, it appears that these changes are based on more refined cost data than was available when our estimate was developed. We believe those changes are reasonable.

- Benefits calculation--The revised estimate uses a 16 percent rate for fringe benefits in FY87 and FY88 and 20 percent for FY88-96 while our estimate used a 27.6 percent rate for all years. We understand that this change has been made based on internal VA budget guidance. We have no problems with that approach for budget purposes, however, we prefer to use the higher percentage for comparison purposes (reflecting Federal rather than just VA costs and adjusted to 34.35 percent to reflect the latest cost OMB guidance on fringe benefit costs provided in OMB Transmittal Bulletin 87-2).

We believe that the changes made are reasonable based on data available to us and address what we believe to be the most significant criticisms raised by the GAO.

IMPACT ON DHCP AND IHS COST COMPARISON

We have made changes to our IHS and DHCP life cycle cost estimates to determine the impact of these changes Depending on the fringe benefit rate used, the following life cycle cost estimates result:

Fringe Benefit Rates	DHCP ($000)	IHS ($000)	Percent Difference
• 34.35 Percent	$924,880	$1,595,838	73%
• 16 Percent in FY87 20 Percent in FY88-96	$878,215	$1,586,968	81%

These compare with estimates of $777 million for DHCP and $1.496 billion for IHS (a difference of 93 percent) identified in our study.

We do not consider the changes in the DHCP and IHS estimates to significantly affect our conclusion that the DHCP approach will be less costly than the IHS approach. We believe all of the various estimates show a significant cost differential.

We do believe that the changes will have an impact on our comparative effectiveness findings. In our study, we projected that DHCP would be less effective than IHS in providing support services and management support, in part, because of inadequate staff resources. The revised cost estimate assumes a substantial future increase in VAMC and ISC staffing (approximately 30 percent more staff). The increased staff resources can be expected to result in significant improvements in future DHCP support services and management support.

* * * * *

We have attached line item descriptions of the revised IHS and DHCP cost estimates for your review. Attachment 1 shows IHS costs using a 34.35 percent benefit rate, attachment 2 shows IHS costs using a 16 percent rate for FY87 and 20 percent rate for FY88-96, and attachment 3 shows DHCP costs using a 34.35 percent benefit rate. The DHCP cost estimate has been provided using your line item categories to facilitate your review. If you should have any questions or require any additional assistance, please do not hesitate to call me at (301) 951-2918.

Sincerely,

BOOZ, ALLEN & HAMILTON, Inc.

Daniel I. Swedberg
Senior Associate

Attachment

Attachment 1
SUMMARY OF IHS
LIFE CYCLE COSTS

29-May-87

	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	TOTAL
PROGRAM MANAGEMENT											$0
CONTRACTOR	$0	$0	$675,000	$675,000	$675,000	$675,000	$450,000	$450,000	$450,000	$450,000	$4,500,000
GOVT	$765,060	$860,568	$960,075	$960,075	$960,075	$960,075	$960,075	$960,075	$960,075	$960,075	$9,306,230
SYSTEM ENGINEERING											$0
HARDWARE	$0	$0	$71,162,791	$94,883,721	$94,883,721	$79,069,767	$0	$0	$0	$0	$340,000,000
SOFTWARE	$0	$0	$16,303,067	$25,938,036	$31,538,854	$33,516,769	$20,069,599	$20,069,599	$20,069,599	$20,069,599	$187,575,120
INSTALLATION	$0	$0	$3,564,000	$17,820,000	$19,008,000	$19,008,000	$11,880,000	$0	$0	$0	$71,280,000
APPL CORD			$17,267,140	$11,426,247	$11,097,697	$7,410,633	$6,790,038	$6,790,038	$6,790,038	$6,790,038	$74,361,871
TRANSPORTATION	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
OPERATIONS											$0
FTE	$0	$0	$3,564,000	$21,384,000	$40,392,000	$59,400,000	$68,112,000	$68,112,000	$68,112,000	$68,112,000	$397,188,000
SUPPLIES	$0	$0	$899,917	$2,761,740	$4,663,739	$6,445,874	$6,887,164	$6,887,164	$6,887,164	$6,887,164	$42,339,924
RECORDING MEDIA	$0	$0	$418,605	$579,070	$606,977	$541,860	$100,000	$100,000	$100,000	$100,000	$2,546,512
DATA CENTER	$0	$0	$792,000	$1,056,000	$1,254,000	$1,254,000	$1,254,000	$1,254,000	$1,254,000	$1,254,000	$9,372,000
POWER&COOLING	$0	$0	$135,000	$810,000	$1,530,000	$2,250,000	$2,580,000	$2,580,000	$2,580,000	$2,580,000	$15,045,000
TELECOM	$0	$0	$1,650,000	$1,650,000	$1,650,000	$1,650,000	$1,650,000	$1,650,000	$1,650,000	$1,650,000	$13,200,000
MAINTENANCE											$0
HARDWARE	$0	$0	$6,753,211	$22,510,704	$40,519,267	$57,027,116	$64,530,684	$64,530,684	$64,530,684	$64,530,684	$384,933,032
SOFTWARE	$0	$0	$594,000	$858,000	$990,000	$1,188,000	$1,188,000	$1,188,000	$990,000	$858,000	$7,854,000
SW ENH	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
TRAIN/DOC	$0	$0	$1,056,000	$1,056,000	$1,056,000	$1,056,000	$528,000	$528,000	$528,000	$528,000	$6,336,000
SITE PREP	$0	$0	$30,000,000	$0	$0	$0	$0	$0	$0	$0	$30,000,000
											$0
											$0
TOTAL	$765,060	$860,568	$155,794,805	$204,368,592	$250,845,330	$271,453,095	$186,979,560	$175,099,560	$174,901,560	$174,769,560	$1,595,837,689

* Federal personnel costs reflect an assumed 34.35 percent fringe benefit rate.

Attachment 2
SUMMARY OF IHS
LIFE CYCLE COSTS

29-May-87

	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	TOTAL
PROGRAM MANAGEMENT											$0
CONTRACTOR	$0	$0	$675,000	$675,000	$675,000	$675,000	$450,000	$450,000	$450,000	$450,000	$4,500,000
GOVT	$669,444	$776,447	$866,608	$866,608	$866,608	$866,608	$866,608	$866,608	$866,608	$866,608	$8,378,755
SYSTEM ENGINEERING											$0
HARDWARE	$0	$0	$71,162,791	$94,883,721	$94,883,721	$79,069,767	$0	$0	$0	$0	$340,000,000
SOFTWARE	$0	$0	$16,303,067	$25,938,036	$31,538,854	$33,516,769	$20,069,599	$20,069,599	$20,069,599	$20,069,599	$187,575,120
INSTALLATION	$0	$0	$3,564,000	$17,820,000	$19,008,000	$19,008,000	$11,880,000	$0	$0	$0	$71,280,000
APPL CORD	$0	$0	$15,422,827	$10,205,803	$9,912,346	$6,619,799	$6,064,790	$6,064,790	$6,064,790	$6,064,790	$66,419,227
TRANSPORTATION	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
OPERATIONS											$0
FTE	$0	$0	$3,564,000	$21,384,000	$40,392,000	$59,400,000	$68,112,000	$68,112,000	$68,112,000	$68,112,000	$397,188,000
SUPPLIES	$0	$0	$899,917	$2,761,740	$4,603,739	$6,445,874	$6,887,164	$6,887,164	$6,887,164	$6,887,164	$42,369,924
RECORDING MEDIA	$0	$0	$418,605	$579,070	$606,977	$541,860	$100,000	$100,000	$100,000	$100,000	$2,546,512
DATA CENTER	$0	$0	$792,000	$1,056,000	$1,254,000	$1,254,000	$1,254,000	$1,254,000	$1,254,000	$1,254,000	$9,372,000
POWER&COOLING	$0	$0	$135,000	$810,000	$1,530,000	$2,250,000	$2,580,000	$2,580,000	$2,580,000	$2,580,000	$15,045,000
TELECOM	$0	$0	$1,650,000	$1,650,000	$1,650,000	$1,650,000	$1,650,000	$1,650,000	$1,650,000	$1,650,000	$13,200,000
MAINTENANCE											$0
HARDWARE	$0	$0	$6,753,211	$22,510,704	$40,519,267	$57,027,116	$64,530,684	$64,530,684	$64,530,684	$64,530,684	$384,955,053
SOFTWARE	$0	$0	$594,000	$858,000	$990,000	$1,188,000	$1,188,000	$1,188,000	$990,000	$858,000	$7,854,000
SW ENH	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
TRAIN/DOC	$0	$0	$1,056,000	$1,056,000	$1,056,000	$1,056,000	$528,000	$528,000	$528,000	$528,000	$6,336,000
SITE PREP	$0	$0	$30,000,000	$0	$0	$0	$0	$0	$0	$0	$30,000,000
											$0
											$0
TOTAL	$669,444	$776,447	$157,857,025	$203,054,681	$249,566,511	$270,568,094	$186,160,845	$174,280,845	$174,082,845	$173,950,845	$1,586,967,586

* Federal personnel costs reflect an assumed 16 percent fringe benefit rate in FY1987 and 20 percent in FY1988-96.

Attachment 3
SUMMARY OF DHCP
LIFE CYCLE COSTS
($000's)

25-May-87

COST COMPONENT	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	TOTAL
VACO FTEE	16	18	20	20	20	20	20	20	20	20	0
VACO PAY & BENEFITS	521	588	651	651	651	651	651	651	651	651	6,215
VACO FRINGE BENEFITS*	179	201	224	224	224	224	224	224	224	224	2,169
VAMC FTEE	395	467	549	635	716	812	852	852	852	852	0
VAMC PAY & BENEFITS	9,587	11,331	13,459	15,796	17,996	20,605	21,692	21,692	21,692	21,692	175,537
VAMC FRINGE BENEFITS*	3,292	3,892	4,622	5,426	6,182	7,078	7,451	7,451	7,451	7,451	60,297
ISC FTEE	236	261	261	261	261	261	260	260	259	259	0
ISC PAY & BENEFITS	6,986	7,769	7,769	7,769	7,769	7,769	7,752	7,736	7,720	7,703	76,742
ISC FRINGE BENEFITS*	2,400	2,669	2,669	2,669	2,669	2,669	2,663	2,657	2,652	2,646	26,361
SIUG FTEE	10	10	10	10	10	10	10	10	10	10	0
SIUG PAY & BENEFITS	326	326	326	326	326	326	326	326	326	326	3,260
SIUG FRINGE BENEFITS*	112	112	112	112	112	112	112	112	112	112	1,120
APP COOR FTEE	203	204	291	280	225	185	178	178	178	178	0
APP COOR PAY & BENEFITS	5,510	5,535	7,885	7,609	6,105	5,030	4,816	4,816	4,816	4,816	56,946
APP COOR FRINGE BENEFITS*	1,893	1,903	2,710	2,614	2,097	1,728	1,654	1,654	1,654	1,654	19,561
PROG TRAVEL	947	1,088	1,210	1,338	1,459	1,603	1,662	1,661	1,660	1,660	14,284
TRAINING TRAVEL	49	41	78	104	92	84	69	69	69	69	724
SIUG TRAVEL	26	26	26	26	26	26	26	26	26	26	260
SOFTWARE MAINT	1,090	1,090	1,547	1,807	2,185	2,185	2,101	2,078	2,127	2,163	18,373
HARDWARE MAINT	9,836	9,836	14,038	16,430	19,910	19,910	19,148	18,184	17,655	17,451	162,398
MISC CONTRACTS	1,286	1,344	1,744	1,708	1,708	1,708	1,705	1,701	1,697	1,694	15,895
FED TRNG	122	102	194	257	228	208	170	170	170	170	1,791
COMMERCIAL TRNG	168	268	268	268	268	268	268	268	268	268	2,580
RECORDING MEDIA	372	212	1,109	823	1,136	435	435	435	435	435	5,858
OPERATING SUPPLIES	3,115	3,115	4,459	5,224	6,337	6,337	6,337	6,337	6,337	6,337	53,935
TELECOM	697	896	1,207	1,485	1,650	1,650	1,650	1,650	1,650	1,650	14,185
UTILITIES	1,040	1,336	1,801	2,215	2,460	2,460	2,460	2,460	2,460	2,460	21,152
ADDL EQUIP	35,018	19,932	29,000	0	0	0	19,047	24,110	13,220	5,098	145,425
REPLACEMT EQUIP	538	578	819	959	1,162	1,162	1,113	1,106	1,131	1,150	9,712
SITE PREP	15,000	15,000	0	0	0	0	0	0	0	0	30,000
TOTAL	100,091	89,191	97,564	75,849	83,741	84,227	103,536	107,574	96,203	87,996	924,880
CUMULATIVE	100,091	189,282	286,846	362,695	446,436	529,660	633,196	740,771	836,974	924,880	

* Calculated using 34.25% fringe benefit factor to reflect total cost to the government (see OMB Transmittal Bulletin 87-2 for rate components).

Requests for copies of GAO reports should be sent to:

U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are $2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.