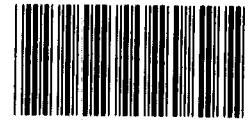# GAO

Report to the Chairman, Committee on Merchant Marine and Fisheries, House of Representatives

April 1990

COAST GUARD

Strategic Focus Needed to Improve Information Resources Management

141250

GAO

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

Information Management and
Technology Division

B-223777

April 24, 1990

The Honorable Walter Jones
Chairman, Committee on Merchant
    Marine and Fisheries,
House of Representatives

Dear Mr. Chairman:

On June 7, 1989, you requested a review of the Coast Guard's manage-
ment of major automated systems in light of its past problems imple-
menting such systems. After subsequent meetings with your office, we
agreed to review the general decision-making framework used for infor-
mation resources management (IRM) at the Coast Guard and identify spe-
cific issues regarding automated systems design, development, and
review. This report responds to your request.

Results in Brief

The Coast Guard has difficulties getting basic information that it needs
to carry out its operations. Whether it is justifying vessel boardings,
responding to oil spills, closing facilities in response to budget cuts, or
tracking hazardous waste violations at its own stations, the Coast Guard
needs, but in many cases does not have, accurate and timely informa-
tion. As the Coast Guard's duties expand and its budget and resources
remain constrained, the role of information technology will become
increasingly vital. The Coast Guards' ability to accomplish its missions
depends on its ability to implement information systems that serve the
needs of the organization overall.

In recognition of the need for better information, the Coast Guard plans
to spend millions of dollars to modernize or replace many major com-
puter systems. Most of the new systems will not be operational until the
mid-1990s and will continue to serve the Coast Guard into the 21st cen-
tury. Because many of these efforts are still in a planning stage, the pre-
sent time offers a key opportunity for determining whether the systems
will meet not only current needs, but future needs as well.

We found several weaknesses that contribute to the Coast Guard's cur-
rent information resources management problems. First, top-level lead-
ership and planning in IRM is lacking. Without top management's
leadership and support, the designated senior official for IRM cannot
ensure that information systems will serve the Coast Guard's long-range
plans. Second, the absence of a strategic IRM plan makes it difficult to

ensure that ongoing and proposed systems development projects logically support agency missions and goals. A strategic IRM plan would address ways that information resources and technology meet administrative and programmatic issues facing the Coast Guard in the short and long terms. Third, the evaluation, development, implementation, and review of information systems is jeopardized by a lack of IRM policies, standards, and procedures. If left unresolved, these weaknesses pose substantial risks to the success of the ongoing systems modernization.

We recommend that the Coast Guard establish a solid IRM framework that corrects these three weaknesses. This framework should contain factors such as the support of an organization's top management, a clearly articulated vision of how technology can help the organization achieve its objectives, and a concrete plan for implementing this vision.[1] By creating this framework the Coast Guard will be in a better position to identify and obtain the information it needs to accomplish its missions.

Information Is Critical to Performing in a Multimission Environment

During the 1980s, the Coast Guard acquired new, expanded responsibilities—most notably drug enforcement and defense-related activities—in addition to its traditional missions of search and rescue, marine environmental protection, law enforcement, and defense readiness. In this multimission environment, the Coast Guard depends on getting large amounts of information, getting it accurately, and getting it on time. In many cases, however, information is not collected, readily available, or easily transferable among various Coast Guard units. These problems have affected both program operations and program management.

The Coast Guard's law enforcement program, for example, suffers from a lack of readily accessible information necessary to support tactical decision-making. In deciding whether or not to board a vessel, timely access to information such as prior boardings or violations is essential to improving law enforcement. Currently, the Coast Guard acknowledges that it may take several hours to retrieve this information from systems within and outside of the Coast Guard.

---

[1] These concepts were reinforced by leaders from industry, the Congress, and executive agencies at a GAO symposium on information technology in October 1989. See Meeting the Government's Technology Challenge: Results of a GAO Symposium (GAO/IMTEC-90-23, Feb. 1990).

Some operations conducted under the Coast Guard's marine safety program also suffer from a lack of information. In a recent report, GAO found that the Coast Guard's oil spill contingency plans in New York and Philadelphia do not contain specific information on how spills of various sizes would be handled with available resources.[2] This type of information is essential for decisionmakers at an oil spill site. In the Exxon Valdez incident, the lack of such information contributed to the Coast Guard's inability to respond effectively.[3]

In addition to needing information for operations, the Coast Guard needs information to support program management decisions. For example, in a November 1988 report on the closing of two Vessel Traffic Service facilities, GAO concluded that the Coast Guard acted primarily to resolve its immediate problem of reducing operating expenses, and gave little consideration to the effectiveness of each of the facilities in enhancing vessel safety in waterways and ports.[4] The Coast Guard could not assess whether it made the correct decision because Vessel Traffic Service safety and cost effectiveness information was not used, was seriously out of date, or was not maintained. Furthermore, GAO's testimony on the Coast Guard's cleanup of hazardous waste sites pointed out that the Coast Guard does not routinely collect and summarize data on environmental violations and the related costs of noncompliance at its own facilities that handle hazardous waste.[5] Without this information, the Coast Guard will find it difficult to project with precision the long-term funding needs for correcting violations of existing regulations.

Information Problems Persist Despite Significant Systems Investments

The Coast Guard is aware of its problems with information technology, and in the past 6 years has spent over half a billion dollars on the development, purchase, operation, and maintenance of and personnel for its information systems. Despite this investment, major automated information systems serving critical Coast Guard missions continue to have problems that affect mission support and impede program operations and management. (See appendix II for examples.)

[2]Coast Guard: Preparation and Response for Oil Spills in Philadelphia and New York Ports (GAO/RCED-90-83, Jan. 26, 1990).

[3]Coast Guard: Adequacy of Preparation and Response to Exxon Valdez Oil Spill (GAO/RCED-90-44, Oct. 30, 1989).

[4]Coast Guard: Better Information Needed Before Deciding on Facility Closings (GAO/RCED-89-48, Nov. 29, 1988).

[5]The Coast Guard's Cleanup of Hazardous Waste Sites (GAO/T-RCED-90-6, Nov. 1, 1989).

Many of the Coast Guard's information systems were developed to support narrow program needs. Most systems are not integrated and cannot share information with other existing Coast Guard systems. In our review of Coast Guard systems documentation and through interviews with project managers, we found several common problems that have led to an inability to retrieve, access, send, or receive information, or determine its accuracy or completeness. For example, field offices sometimes have to use several different systems to obtain information on the variety of interrelated tasks they are performing. (See appendix II for details.)

Systems Modernization Efforts Are Focused on Correcting Technology Problems

The Coast Guard plans to invest millions of dollars in the next few years modernizing or replacing many major computer systems to eliminate shortcomings with existing information systems technology. Most of these efforts are in an early planning or development stage, and are expected to be operational within the next 2 to 5 years. (See appendix III.)

In examining several ongoing systems replacement or enhancement efforts, we found that the Coast Guard is focusing on technology-related solutions without reassessing the basic purposes and uses of its information systems. The technological solutions may correct some existing problems with data access, storage, retrieval, and exchange, but will not help the Coast Guard to respond to organizationwide information needs in fundamentally new and different ways. For instance, new hardware and software may overcome many existing shortcomings with information systems performance caused by equipment obsolescence and inflexible software applications. Also, plans to apply open systems information processing standards, in accordance with federal policies, through an information architecture can help ensure that current systems interoperability problems are addressed.

These are positive steps, but other important issues related to the success of the Coast Guard's systems modernization efforts remain largely unaddressed. Organizationwide reassessments of the needs, purposes, and uses for information—all critical to improving present and future mission performance—are not occurring concurrently with new technology plans.

Underlying Causes of Coast Guard Information Problems

Defining an agency's information needs and acquiring the information technology to support these needs requires careful, agencywide planning. In reviewing the Coast Guard's IRM program, we found three interrelated problems that pose risks to the success of the Coast Guard's computer modernization efforts and hinder the Coast Guard's ability to identify its current and future information needs. First, top-level leadership and planning in IRM is lacking. Second, the absence of a strategic IRM plan makes it difficult to ensure that ongoing and proposed systems development projects logically support agency missions and goals. Third, the evaluation, development, implementation, and review of information systems is jeopardized by a lack of IRM policies, standards, and procedures.

Defining the Role of Information Technology: Top Leadership and Vision Needed

Top leaders in the Coast Guard periodically analyze new and long-term strategic, administrative, and programmatic issues facing the organization. The Commandant issues a Long Range View every 2 years that assesses the Coast Guard's current missions and how these are likely to change or broaden during the next several years. This document provides broad policy guidance for program offices during the Planning, Programming, and Budgeting System's cycle that determines priorities for resource needs and allocations. In 1989, the Commandant created a Strategic Planning Council to assist him in strategic, long-term planning by examining how Coast Guard missions could be affected by changes in the agency's internal and external environment.

In our review of the most recent Long Range View and our discussions with the head of the Strategic Planning Council, we found that the role of information, information technology, and other related resources in addressing strategic, administrative, and programmatic issues is not clearly addressed. Neither the Long Range View nor the Strategic Planning Council indicate how the organization will respond to current or future strategic issues in terms of information requirements and the uses of information technology.

This lack of top management vision on the use of information technology reflects the existing philosophy of the Coast Guard's leadership. IRM guidance and direction is not viewed as a top management function by Coast Guard leaders. In 1988, the Commandant delegated responsibilities for IRM direction, guidance, and control to the Admiral who heads the Office of Command, Control, and Communications (C³). Although the C³ Admiral is the designated senior IRM official, we found he has great difficulty providing agencywide IRM leadership, in part because he lacks

sufficient authority to do so. In a September 1989 memo to the Chief of Staff, the C³ Admiral acknowledged this dilemma, noting that his designation as the senior IRM official has been a classic case of responsibility without authority. Our interviews with some program officials indicated that C³ has had difficulty gaining acceptance by other Coast Guard offices of its IRM leadership role. Its organizational status is equivalent to the program offices, and it is these offices that have direct responsibility for the information systems supporting their work. Only recently have C³ officials been involved, informally, in the Coast Guard's budget development process. The absence of strong IRM leadership within the Coast Guard management's highly decentralized environment relegates C³ to a support office with a reactive rather than a proactive IRM role.

This lack of leadership is exemplified by the senior IRM official's inability to effectively integrate IRM projects with the existing Coast Guard process used to allocate resources. For example, C³ has recognized that more efficient information management is necessary to support operational decision-making. C³ proposed an Operations Information System prototype to enhance the command and control functions of a wide variety of Coast Guard decisionmakers. This system would merge crosscutting information from existing automated systems supporting various operational missions, such as search and rescue, law enforcement, defense operations, and intelligence. Three Coast Guard operation program offices reviewed the proposal and agreed that the project was essential to improving performance. The head of the Office of Engineering and Development also concurred, and had the Research and Development Center in Groton, Connecticut, develop a project plan to analyze requirements and the prototype's design.

Over a year later, little progress has been made on this project. Officials at the Coast Guard's Research and Development Center stated that more immediate problems with existing automated systems have demanded management's attention and consumed existing staff resources. For the Operations Information System project to receive higher priority, they indicated, it must receive backing from top Coast Guard management.

Strategic IRM Plan Needed to Articulate the Information Technology Vision

A strategic IRM plan provides the mechanism to set and evaluate priorities and specifies how an agency's information technology will support its mission. This process should provide the vital link between an organization's business strategy and its information assets and resources. Office of Management and Budget Circular A-130 specifically requires

federal agencies to establish a multiyear strategic planning process for acquiring and operating information technology that meets program and mission needs, reflects budget constraints, and forms the basis for budget requests. The Coast Guard does not have a strategic IRM plan, and does not engage in long-range IRM planning as part of its Long Range Planning Cycle. Several Coast Guard officials explained that such planning has not been undertaken because senior Coast Guard management views information technology as a traditional data processing support function, not as a strategic resource.

Without a strategic IRM plan, attempts to solve the Coast Guard's information problems are uncoordinated and driven by individual program needs. For example, the C^3 office realizes the need for a standardized, Coast Guard-wide data dictionary.[6] The Corporate Database Project is being used to construct this dictionary over time. However, this project is not coordinated with other systems development projects in the program offices, many of which are scheduled for implementation before the Corporate Database project is completed. Thus, new systems being developed through the Coast Guard's modernization effort run the risk of continuing to function as stand-alone systems, despite integrated operational and managerial information needs that exist across organizational boundaries.

In the absence of IRM strategic planning by the Coast Guard's top officials, the Coast Guard uses its budget planning and review process to rank and scrutinize ADP procurements. This practice presents two problems for decisions made about information systems projects. First, funding decisions continue to be based on the specific needs of individual Coast Guard offices. With C^3 involved only informally in the budget review process, a comprehensive, coordinated, and agencywide perspective on information systems projects is difficult to achieve. Without this perspective, the Coast Guard's top leadership cannot ensure that information resources are being planned, managed, and used in the most effective manner agencywide.

Second, it is difficult for the budget review process to ensure that systems requesting funding have been adequately planned. Cases exist where software development and hardware acquisitions have been funded prior to sufficient systems requirements analysis, definition, or design. For example, inadequate system development planning for the

---

[6]When different systems are to share data, plans should define standard data elements that will be common across all systems and specify procedures for managing and sharing the data.

Automated Mutual Vessel Emergency Rescue System—used to support Coast Guard search and rescue operations—was not recognized by budget review staff until almost one year after system redesign efforts had been funded. As a result, the project schedule slipped, costs increased, and better support for search and rescue operations was further delayed. The same problem recently surfaced with the redesign of the Coast Guard's Law Enforcement Information System; however, 1991 funding for system redevelopment was delayed until more complete systems design and requirements analyses were completed. In short, the budget review process is being used to perform a technical function for which it is not well suited, namely, to scrutinize systems design and development proposals.

During the course of our review, the Coast Guard took steps to change the funding and development of information systems to better assure that projects are adequately planned before they are funded. A Project Development Board comprised of representatives from the Chief of Staff, C^3, and several major program offices has been created to review and approve major hardware and software acquisitions prior to consideration of funding. The Coast Guard's Research and Development Center will play a key role in system developments and will be responsible for directing the new system design efforts approved by the Board and funded through the budget approval processes. These changes are constructive, but they effectively address only some of the risks associated with the funding of inadequately defined and designed systems proposals, and do not address, for example, the risks associated with a lack of standards and procedures for developing automated systems.

Policies, Standards, and Procedures Needed to Anchor IRM

Policies, standards, and procedures can provide stability to an IRM program, particularly to development efforts, by ensuring that these efforts follow a strategic plan. IRM policies ensure that agencywide initiatives, such as IRM management control, review, and approval are effectively implemented throughout the agency. System development standards and procedures can provide guidelines for individual development projects. However, this potential stability is missing since the Coast Guard has not developed comprehensive IRM guidance.

The Coast Guard's senior IRM official has responsibility for implementing IRM policies, standards, and procedures. As in the case with strategic planning, IRM policies have not been clearly articulated by top management, or the C^3 office. Promulgation of IRM standards and procedures has over the past 3 years been limited to only one IRM directive addressing

systems developments.[7] It specifies that a proposal summarizing certain early, standard, life cycle requirements—such as resource requirements, benefits and costs, organizational and user impact, and alternatives analyses—be approved by C³ for cross-unit automated systems that exceed certain cost thresholds. C³ officials acknowledged that a lack of resources has hindered efforts to formulate standards, but explained that an informal process to disseminate applicable governmentwide standards has been created.

The lack of formal IRM policies, standards, and procedures increases the risk that development projects will not meet the Coast Guard's needs. In discussions with various project managers, we found that a distinct disparity exists in the way systems are developed. Some project managers are cognizant of governmentwide standards and apply them to their system development efforts, while others rely on the C³ office to provide them what they need. This office reviews proposals that summarize the results of early life cycle documentation, approves system development proposals based on this review, and, in some cases, participates in the development. However, it is not responsible for evaluating system justifications. The program office is responsible for project oversight, reviewing feasibility studies and requirements analyses, and determining the most beneficial way to develop IRM resources. System development risks increase because C³'s oversight is largely informal once projects are approved for funding.

The Coast Guard's C³ office is in the process of creating an information technology architecture to provide a standard framework that governs the deployment and use of information technology resources. For example, the technology architecture will establish standards for the use of hardware, operating systems, and telecommunication protocols. However, the formulation of this architecture suffers from the lack of guidance that an IRM plan and policies would provide. For example, it is not clear that the completed components of the technology architecture have fully addressed mission objectives of current and future Coast Guard systems, and the manner in which these systems will be employed. If such systems are to be integrated and share data, the architecture should define standard data elements, a data dictionary, and detailed characteristics of database management systems. In addition, a process for adequately testing, implementing, and enforcing the architecture has not been set up.

---

[7]Commandant Instruction 5231.2, Planning Approval for Automated Information Systems (AIS) (May 15, 1988).

Management of Information Resources: Creating a Framework Contributes to Success

The Coast Guard's increased responsibilities and expanded mission combined with its constrained budget and resources puts great pressure on the agency to make sound, cost-effective decisions and justifiable funding requests. Put in this perspective, the Coast Guard's effective management of its information and technology is of critical importance. The agency is entering a period of modernization designed to meet new or expanding responsibilities while operating under budgetary constraints, which poses a formidable challenge to the Coast Guard's management.

Ways of meeting such challenges are currently being studied by policymakers both in private industry and the government. In a recent GAO symposium, "Meeting the Government's Technology Challenge," leaders from industry, the Congress, and the executive agencies agreed on several principles that make up a framework to guide the effective acquisition and management of information technology. Many of the underlying principles of this framework reinforce our work at the Coast Guard by emphasizing the significance of committed leadership, a clearly articulated vision of how technology can be used to serve an agency's objectives, and a concrete plan for implementing this vision.

Conclusions

At present, the Coast Guard lacks a clear vision of how it can benefit from information technology, and without this understanding IRM initiatives tend to focus only on the needs of individual units. A comprehensive, agencywide focus could extend beyond automating existing processes and procedures, to developing new ways of accomplishing objectives.

An absence of leadership places all of the Coast Guard's information technology initiatives at risk. No strategic IRM plan exists to guide the agency during this period of intense modernization. At present, IRM planning is not even required at the program-office level. The danger exists that systems resulting from this modernization will continue to be a loose collection of unrelated projects. Without interconnected and compatible systems, the Coast Guard will still find it difficult to obtain information in a timely, convenient, and economical fashion.

Some of these concerns may be alleviated by an information architecture that the Coast Guard is implementing. Although the architecture should reduce the likelihood of acquiring incompatible technology, it is not tied to any strategic vision, nor is there any clear provision for implementing or enforcing it throughout the agency. The architecture represents a step in the right direction, but it does not in itself provide

the comprehensive IRM policies and procedures or systems development standards that the Coast Guard needs to guide the modernization of its information systems.

The involvement of the Coast Guard's new Project Development Board and subsequent use of Research and Development staff in determining requirements and designing systems may also help to produce improved systems within realistic time frames. However, no official directive outlining the authority and purpose of the Project Development Board has been promulgated by the Commandant. Without proper delegation of authority and a long-term information resources management plan, neither the Board nor the Research and Development Center can provide strategic policy direction on the desired role and use of information technology. Setting priorities for agencywide automated information systems could also be difficult. As a consequence of these limitations, both serve as reactive bodies, responding to and reviewing information system needs on a project-by-project basis.

Recommendations

The Coast Guard's top-level management must become fully involved in the IRM decision-making process if the agency is to have the information it needs to accomplish its missions. We therefore recommend that the Secretary of Transportation direct the Commandant of the United States Coast Guard to clarify the role and authority of the senior IRM official and restructure the way in which the agency is managing the modernization of its information systems. The restructuring should include a clear statement of the agency's needs and the ways in which information technology can serve these needs, a strategic IRM plan that supports this view, and comprehensive policies, standards, and procedures to guide implementation.

It is up to the Commandant to determine the most effective way of ensuring top-management involvement in IRM. One option he should consider is to create a centralized IRM steering committee comprised of the Coast Guard's top management to provide direction for IRM strategic planning, policy, and procedures. This committee could be supported by an IRM advisory committee made up of program and project managers, technical staff, and system end-users to make policy recommendations, develop procedures, and develop recommendations on operational standards. Whatever option he chooses, he and his Chief of Staff should give the IRM decision-making process direction and solid support.

Agency Comments and Our Evaluation

In commenting on the report, Department of Transportation officials told us they agree with our findings and recommendations, specifically recognizing the need for improvement in the IRM strategic planning process. They indicated that our report findings and recommendations would be used as a benchmark in reviewing IRM in the Coast Guard and other agencies within the Department. They also submitted the Coast Guard's written response to the Secretary of Transportation as part of the official agency comments.
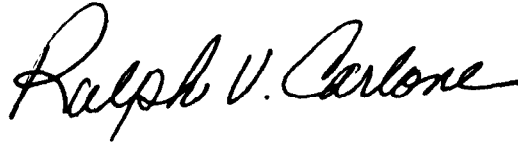
In its written response to the report, the Coast Guard agreed with the need to develop a strategic IRM plan and an IRM planning process. With regard to the need for comprehensive IRM guidelines, the Coast Guard stated that it would promulgate some additional IRM policies, standards, and procedures. The Coast Guard did not agree that top-level management has not been involved in IRM planning, guidance, and direction, citing the establishment of the C^3 office, which has responsibility for managing the agency's information resources, and, citing other examples of involvement and vision. The Coast Guard did not specifically respond to the recommendations to clarify the role of the designated senior IRM official and to determine the way in which top management will be involved in managing information resources. However, the Coast Guard commented that it has already started a program to provide top management education on the strategic opportunities provided by information technology, and has contracted for services to facilitate an organizationwide assessment of information needs.

In light of the Coast Guard's current systems modernization and future information needs, we believe that by not acting on all of our recommendations, the Coast Guard only perpetuates risks that our recommendations are designed to reduce. With the support and commitment of top management, the Coast Guard should seek more comprehensive and detailed solutions to its IRM shortcomings, explicitly addressing issues concerning the involvement of top management, the role and authority of its senior IRM official, and the implementation of IRM policies, standards, and procedures to guide the acquisition, management, and oversight of its information system projects. Such steps could provide the necessary framework for effectively managing its information resources.

The Coast Guard's comments on the report and our evaluation of these comments are contained in appendix IV.

As arranged with your office, we plan to publicly release this report at the time of its issuance. At that time, we will send copies to the Secretary of Transportation, the Commandant of the United States Coast Guard, and other interested parties. This report was prepared under the direction of JayEtta Hecker, Director, Resources, Community, and Economic Development Information Systems, who can be reached at (202) 275-9675. Other major contributors are listed in appendix V.

Sincerely yours,

Ralph V. Carlone
Assistant Comptroller General

Contents

Abbreviations

AMIS	Acquisition Management Information Systems
AMMIS	Aviation Maintenance Management Information System
ARSC	Aviation Repair and Supply Center
C^3	Office of Command, Control, and Communications
CDB	Corporate Database
GAO	General Accounting Office
IMTEC	Information Management and Technology Division
IRM	Information Resource Management
LEIS	Law Enforcement Information System
MSIS	Marine Safety Information System
PAMIS	Personnel Assignment Management Information System
PDS	Personnel Data/Decision System
SAR	Search and Rescue Database System
SARMIS	Search and Rescue Management Information System
VIIS	Vessel Identification Information System

Objectives, Scope, and Methodology

The objective of our review was to determine the adequacy of (1) the general decision-making framework used at the Coast Guard to approve automated information projects, develop IRM polices and procedures, and direct planning for long-term informational needs, and (2) identify specific automated systems issues regarding systems design, development, and review. We conducted our work from July through November 1989 at the Coast Guard Headquarters in Washington, D.C.; the Coast Guard Research and Development Center in Groton, Connecticut; and the Department of Transportation in Washington, D.C.

At Transportation's Office of the Secretary, we interviewed the Director of the Office of Information Resources Management and analysts from the IRM and Acquisition Offices. At the Coast Guard, we interviewed Chief of Staff programming, planning, and policy officials; the designated senior IRM official; other IRM officials; program and project managers; and officials at the Research and Development Center. We also reviewed Coast Guard policy, planning, budget, and system justification documents, and relevant reports and legislative documents. We interviewed a consultant from Index Group, Incorporated, who was responsible for assisting the Coast Guard in its development of an information architecture. To assist in our evaluation of the Coast Guard's IRM program, we also contracted with an IRM consultant. In addition, we selected and reviewed eight Coast Guard information systems that were (1) identified by the Coast Guard as being critical to the accomplishment of Coast Guard missions, (2) listed in different program areas and were at different stages of development, and (3) budgeted as some of the Coast Guard's most costly system developments. As part of our systems review, we developed indicators to assess the risk that systems development projects will not meet Coast Guard needs. Problems with existing systems are contained in appendix II and concerns about several ongoing systems enhancements, replacements, or developments are discussed in appendix III.

Our work was performed in accordance with generally accepted government auditing standards. The Department of Transportation provided oral comments and presented the Coast Guard's written response to the Secretary as part of the official agency comments. These comments are summarized and evaluated in the body of this report, and the Coast Guard's written response and our evaluation is included in its entirety in appendix IV.

Common Problems With Existing Coast Guard Systems

In our review of Coast Guard systems documentation and through interviews with project managers, we found several common problems that reduced the systems effectiveness and efficiency in supporting the Coast Guard's mission objectives. The Coast Guard's Offices of Marine Safety, Security and Environmental Affairs, Navigation, Safety and Waterway Services, and Law Enforcement and Defense Operations manage most of the agency's operational mission programs, such as marine environmental response, search and rescue, and law enforcement. Each of these offices along with various administrative ones, including the Acquisition, Engineering, and Personnel offices, is supported by separate information systems.

Systems supporting these offices have experienced a variety of problems including limited data query capability, system responsiveness and reliability problems, data transfer and data integrity difficulties, problems with obsolete hardware, and inflexible software applications. Table II.1 summarizes the problems across five Coast Guard systems.

Table II.1: Common Problems With Existing Coast Guard Information Systems

System	Limited query ability	Responsiveness & reliability problems	Data transfer difficulty	Data integrity problems	Hardware & software obsolete
Aircraft Repair and Supply Center System[a]	X	X		X	X
Law Enforcement Information System (LEIS)	X	X	X	X	
Search and Rescue Database System (SAR)	X	X	X	X	
Marine Safety Information System (MSIS)	X	X	X	X	X
Personnel Assignment Management Information System (PAMIS)	X			X	X

[a]This system is actually a collection of several different systems and software applications developed over the last 20 years. These systems will be consolidated into a single, integrated system called the Aviation Maintenance Management Information System (AMMIS).

These five problems have occurred for a variety of reasons. All five of the systems have problems with data integrity. Information received from these systems is unreliable or redundant because of limited system error checking or validation controls, inadequate user procedures, and lack of systems integration. As shown, the systems had limited data query capability, obsolete hardware (poor or nonexistent vendor support), software not meeting current user needs, and system responsiveness and reliability problems.

Data query problems have resulted because end users of some systems, such as the Search and Rescue database (SAR) and management information system (SARMIS) depend upon technical support staff to tailor software programs for certain data requests. Field office staff find the data query process for the Law Enforcement Information System (LEIS) difficult to use, tedious, and time consuming. Data are being provided to the system but rarely extracted to support day-to-day operational decisions.

Hardware problems have occurred because hardware used to support systems such as those associated with the Aircraft Repair and Supply Center (ARSC) is obsolete. The vendor no longer manufactures spare parts for the hardware, and maintenance support for the operating system can only be obtained on an emergency basis. Contractor-developed software applications—designed in the early 1980s or before—are not meeting user needs for several systems, including MSIS, the ARSC systems, and LEIS. Several of the software applications used to manage the databases are difficult to change because they were written by contractors, many of which have inadequate documentation. System responsiveness and reliability problems have interfered with users ability to obtain information from the systems because response times are slow, computers are down, or data are not current.

Data transfer difficulties have occurred for some Coast Guard systems—such as LEIS, SARMIS, and MSIS—because they are not integrated systems. These systems have highly inefficient data transfer processes. For example, many Coast Guard field offices transfer data to District Offices by mailing floppy diskettes or printed reports which are then reentered into another system.

Coast Guard System Modernization Projects

The Coast Guard is in the process of replacing or enhancing many of its automated information systems. Also, several new information systems are in various stages of planning, design, and development. When the costs associated with these systems are viewed collectively and over their life cycle, the IRM investment being made by the Coast Guard over the next 5 years is significant. Almost every major information system is scheduled for redesign, enhancement, or replacement and could be affected by new standards being implemented by the Coast Guard's new information architecture.

After consulting with C³ officials, we selected eight ongoing automated systems projects to determine whether potential risks existed as a consequence of such factors as inadequate systems definition and design, complex requirements, spiraling costs, shortcomings in project management, insufficient user involvement, sophistication of technology involved, and lack of adherence to governmentwide standards. In making these risk determinations, we relied upon official Coast Guard documents and interviews with project managers and C³ personnel. The eight systems we examined (1) were identified by the Coast Guard as being critical to the accomplishment of Coast Guard missions, (2) covered different program areas and were at different stages of development, and (3) included some of the Coast Guard's most costly system developments. Table III.1 summarizes select information about these eight systems projects.

We found a disparity of risk across systems, with some efforts much better defined and managed than others. Our work surfaced two areas of concern which indicated weaknesses in the procedures used by the Coast Guard to direct automated systems development projects through life cycle management processes. While these concerns cannot be generalized to every project, we believe they point to significant agencywide information resources management weaknesses that deserve the Coast Guard's attention.

For some systems, we found incomplete documentation for project development schedules, cost estimates, or system deliverables. This was a particular problem with the Corporate Database (CDB), Search and Rescue Management Information System (SARMIS), and Law Enforcement Information System (LEIS II) projects. In some instances, the current project manager lacked adequate documentation on changes previously made to the existing system. These problems are exacerbated by the lack of sufficient Coast Guard documentation on standard life cycle

management requirements expected of information systems project managers.

A second general area of concern is an apparent lack of coordination between projects. Several new information systems, such as CDB, LEIS II, MSIS II, and VIIS, are expected to interface with other Coast Guard systems or other agency systems. Because these systems are in an early design or requirements stage, available documentation was not specific on how this coordination was to occur. However, it appears projects are being designed to support specific program functions without addressing the need for linkages to other systems to minimize potential data collection redundancies. As these system requirements become more fully defined, the Coast Guard will need to review proposed system linkages carefully to minimize redundancies.

Table III.1: Cost and Planning Schedule for System Modernization Projects

Dollars in millions

System name	Objective	Fiscal year Start date	Fiscal year Complete date	Development cost[a]
Acquisition Management Information System (AMIS)	AMIS is being designed to improve contract management and decision support for major acquisitions.	1987	1992	$6.8
Aviation Maintenance Management Information System (AMMIS)	AMMIS is expected to provide an integrated system to support aviation repair, logistics, and financial and administrative functions at the Aircraft Repair and Supply Center, Coast Guard headquarters, and 26 Coast Guard Air Stations.	1985	1991	8.7
Corporate Data Base (CDB)	CDB is being developed to provide mid-level management with consolidated information from existing systems; it is also expected to provide an agencywide data dictionary.	1988[b]	c	3.0[d]
Law Enforcement Information System II (LEIS II)	LEIS II is expected to provide all users of Coast Guard law enforcement information with data that will support tactical, patrol, and program planning decision making at all organizational levels.	1989	1994	5.8
Marine Safety Information System II (MSIS II)	MSIS II is expected to enhance informational support for Coast Guard's numerous marine safety security functions (e.g., port safety, vessel inspections, merchant vessel documentation, and marine pollution incidents) by increasing system reliability and availability through new software and flexible data processing technology.	1987	1996	20.0[e]
Personnel Data Decision System (PDS)	PDS will replace existing personnel systems (e.g., PAMIS) and provide an electronic backup of service records.	1989	1993	8.5
Search and Rescue Management Information System (SARMIS)	SARMIS is expected to provide a more efficient computerized method to process and communicate Coast Guard search and rescue data.	1984	c	1.6
Vessel Identification Information System (VIIS)	VIIS will modernize the processing of maritime liens and ship mortgages, and will include vessel registration information.	1989	1993	15.6[f]

[a]The Coast Guard does not use a uniform agency document or procedure to estimate or record costs for system development projects. The cost estimates listed here were derived from various project documents provided by Coast Guard officials and our discussions with project managers.

[b]The CDB project was funded under the auspices of the Coast Guard's Distributed Computer System project between fiscal years 1988 and 1990.

[c]Sufficient information not available.

[d]This figure represents budget projections for the period fiscal years 1991 through 1995.

eThis figure represents cost estimates only for the period between fiscal years 1990 and 1996 and includes costs associated with the Vessel Documentation component of MSIS II that is expected to be integrated with the Vessel Identification System component of VIIS. Between fiscal years 1987 and 1989, MSIS II preliminary development costs were funded from operations and maintenance and other existing MSIS accounts.

fThis estimate is for a preferred systems development alternative identified in an internal Coast Guard study. The estimate is based upon the development costs of a similar Department of Transportation computerized information system (Commercial Drivers License Information System) and the Vessel Documentation portion of the MSIS II. During our review, the Coast Guard hired a contractor to perform a more detailed alternatives analysis, which will form the basis for a final design decision.

Agency Comments and Our Evaluation

Memorandum

U.S. Department
of Transportation

**United States
Coast Guard**

Subject GAO REPORT ON STRATEGIC FOCUS NEEDED   Date.   2 0 MAR 1990
TO IMPROVE INFORMATION RESOURCES   7500
MANAGEMENT, GAO/IMTEC-90-32 APRIL 1990

                                            Reply to   G-TIS
From Commandant, U.S. Coast Guard   Attn of   OFFUTT
                                                           267-2996

To Director of Management Planning

1. As requested, the proposed DOT reply to the subject GAO
report is enclosed.

A. BRUCE BERAN
Rear Admiral, U.S. Coast Guard
Chief of Staff

Encl: (1) Proposed DOT statement on GAO report

DEPARTMENT OF TRANSPORTATION
STATEMENT ON GAO REPORT

I.   TITLE: COAST GUARD: Strategic Focus Needed to Improve
     Information Resources Management, GAO/IMTEC-90-32,
     April 1990

II. SUMMARY OF GAO FINDINGS AND RECOMMENDATIONS:

     The GAO report stated that the Coast Guard's ability
     to accomplish its missions depends on its ability to
     implement information systems that serve the needs of the
     organization overall. The GAO found, that while the Coast
     Guard was actively modernizing aging ADP systems and
     automating existing processes, a comprehensive, agency wide
     Information Resources Management (IRM) focus was needed to
     develop new ways of accomplishing agency missions. The
     report found that IRM guidance and direction as well as a
     vision of how technology can help the organization achieve
     its objectives is not viewed as a top management function
     by Coast Guard leaders.

     The GAO report, found as a result of this lack of
     vision, there was a no strategic Coast Guard IRM plan.
     Such a plan should describe how the organization will
     respond to current or future strategic issues in terms of
     information requirements and the uses of information
     technology.

     Finally, the report found that the evaluation,
     development, implementation and review of information
     systems is jeopardized by a lack of IRM policies, standards
     and procedures.

III. SUMMARY OF DEPARTMENT OF TRANSPORTATION POSITION:

     GAO took a snapshot of an agency completing the
     "Initiation and Contagion" stages of ADP growth* and
     entering the "Control and Integration" stages. The Coast
     Guard recognizes that it has reached this critical
     juncture. Coast Guard management attitudes and processes
     have demonstrated responsiveness to the need for change to
     keep pace with the rapid technological growth engendered by
     the computer revolution. In fact, the Coast Guard has
     taken many positive steps toward this objective. The Coast
     Guard has a strong technological foundation and an
     aggressive Command, Control and Communications (C3) staff,

     *"Managing the Crises in Data Processing," Richard L.
     Nolan, Harvard Business Review, March-April, 1979,
     pp. 115-126.

See comment 1

that is well positioned to implement the necessary manage-
ment changes. To insure long term success, these changes
should be modifications of existing processes as opposed to
new processes which often fail due to lack of institutional
commitment.

See comment 2.

The Coast Guard does not agree that top level
management has absented itself from IRM planning, guidance
and direction. The Chief, Office of Command, Control and
Communications is very much a member of top level
management. The very fact that the Commandant established
an Office of Command, Control, and Communications in 1981
is indicative of the Coast Guard's long term commitment to
more visible management of the emerging IRM technology.
The Commandant's delegation of responsibilities for IRM
direction, guidance and control was clearly intended to
draw sharper organizational focus to the integration of IRM
into the fabric of the Coast Guard. Within the last two
years, as IRM has become increasingly recognized as a
critical success factor in nearly every mission area, the
role of the Designated Senior Official has matured, as has
his influence with other Coast Guard offices and his role
in the planning, programming and budgeting processes. Top
level management does indeed have a vision for the
integration of IRM systems throughout the Coast Guard as
evidenced by the broad placement of the Coast Guard
Standard Workstation aboard vessels and every shore unit,
increased emphasis upon source data automation, and
organizational priority given to the modernization and
replacement of mission critical computer systems.

See comment 3.

As the organization prepares to invest significant
resources into the modernization and replacement of several
major computer systems, the Coast Guard takes exception to
the assertion that its focus is upon technology-related
solutions without assessing information needs, purpose and
usage. In particular, the Marine Safety Information System
(MSIS II), the revision of Automated Mutual Vessel Energy
Rescue System (AMVER), Law Enforcement Information System
(LEIS II) have initiated and painstakingly pursued the
requirements analysis process to insure that the systems
will be built to serve both strategic and tactical
informations needs. Each of these projects, as well as the
Corporate Data Base (CDB), were in an evolutionary stage
when first examined by GAO. Adequate documentation
appropriate to the current and planned stages of
development are now available.

See comment 4.

The Coast Guard agrees with the need to develop a
formal strategic IRM plan and intends to promulgate
additional policies, standards, and procedures to guide the
IRM processes. In many cases, however, the underlying
objectives of such formal plans, policies and standards

have already been successfully achieved through strict application of existing Coast Guard, Department of Transportation, and General Services Administration policies, standards, and procedures. For example, the Coast Guard believes that current Sensitive Application Certification processes included in its ADP security program provide adequate control to insure that program managers implement systems properly.

See comment 5

The Coast Guard agrees that the current technology architecture may not have fully addressed mission objectives of current and future Coast Guard Systems. However, development of the technology architecture is a significant starting point. The Coast Guard is presently proceeding with the applications part of the architecture and improving the systems planning process in its FY90 project with the Transportation Systems Center. It should be noted that this architecture is dynamic in nature and will be reviewed at least every two years to insure that it reflects any changes in vision as new uses of information technology emerge.

See comment 6

The Coast Guard recognizes that it has reached a critical phase in adapting IRM technology to better accomplish its organizational objectives. Many of the difficulties indicated in the report have been well known to the Coast Guard; indeed they were the impetus for ongoing modernization and replacement efforts. At the same time, past efforts have resulted in significant accomplishments. The Coast Guard is generally considered among other government agencies to be at the forefront in the application of IRM technology. These successes aside, the Coast Guard acknowledges that there remains room for improvement. The Coast Guard finds the GAO report helpful in identifying areas for additional attention, and also in confirming that many current efforts are headed in the right direction.

IV. STATUS OF CORRECTIVE ACTION:

See comment 7

The Coast Guard has developed and is in the process of promulgating a directive that:

a. Incorporates IRM considerations at all levels of the Planning, Programming and Budgeting process.

b. Requires a strategic IRM plan that includes initiatives that will help the agency meet the challenge of increasing mission responsibilities with level or constrained resources through the use of Information Technology.

c. Links strategic IRM Plans with the priorities of the
   Research and Development Project Development Board.

d. Provides a mechanism for reporting the status of ongoing
   cross functional systems development efforts to top
   management.

   The Coast Guard has already started a program to
provide top management education on the strategic
opportunities provided by information technology and has
contracted for services to facilitate an organization wide
assessment of information needs.

   The Coast Guard has done extensive evaluation of
Information Engineering Workbench (IEW), an advanced
Computer Assisted Software Engineering (CASE) tool and is
implementing many major systems using this technology. In
addition the Coast Guard will implement policies and
procedure for the evaluation, development, implementation
and integration of information systems as follows:

a. Formal adoption of DOD standards for systems development
   and requirements for the use of CASE tools: Summer 1990

b. Implementation of the FIPS Pub 156 (a standard
   Information Resource Dictionary system) and
   requirements for its use: Fall 1990

   The Coast Guard believes that this corrective action
is responsive both to the GAO report and the challenges the
agency is facing in its Information Resources Management
responsibilities.

GAO Comments

1. The Coast Guard stated that its management attitudes and processes have demonstrated a responsiveness to the need for change to keep pace with technological growth, and that it has taken many positive steps in this regard. As an example of these steps, the Coast Guard cited a strong technological foundation and an aggressive Command, Control, and Communications (C^3) staff that is well positioned to implement necessary management changes. The Coast Guard also stated that to ensure long-term success, these changes should be modifications of existing processes as opposed to new processes, which often fail because of a lack of institutional commitment.

We agree that the Coast Guard has taken several positive steps to deal with IRM issues facing the agency. However, as explained on page 4, we found that the Coast Guard's focus over the next few years is directed toward eliminating technology-related problems without a concurrent reassessment of the organization's overall information needs. Without this assessment, the Coast Guard may lose a key opportunity to identify and obtain the information it needs to accomplish its missions.

We believe that the role and authority of the C^3 office has not been clearly delineated, impairing its ability to implement and guide organizationwide IRM policies. As discussed on pages 5 through 7, this office has not been able to provide IRM leadership or effectively solve IRM issues, and it has not been given adequate support by top Coast Guard management. Further, C^3 has been involved only informally in key information system budgeting and oversight processes.

We agree that modifications of existing IRM processes may serve as initial corrective steps for some of the Coast Guard's problems; however, we do not agree that this approach is the solution to the Coast Guard's overall IRM deficiencies. Our findings and recommendations point to the need for changes in management of information resources that transcend changes in processes. With vision, leadership, and commitment from top management, the Coast Guard could develop an IRM philosophy that would unite individual program efforts and address the interrelated problems that pose risks to the success of the Coast Guard's modernization efforts. By not seizing this opportunity to restructure its IRM program, the danger exists that systems resulting from the modernization effort will continue to be a loose collection of unrelated projects.

2. The Coast Guard does not agree that top-level management has absented itself from IRM planning, guidance, and direction. As an example of such involvement, the Coast Guard cited the establishment of the

C³ office, whose chief is a member of top-level management. The Coast Guard also believes that top-level management has a vision for the integration of IRM systems throughout the agency. This vision, according to the Coast Guard, is illustrated by the broad placement of the Coast Guard standard workstation aboard vessels and every shore unit, increased emphasis on source-data automation, and priority given to the modernization and replacement of mission-critical computer systems.

We disagree. The mere presence of top-level management in IRM decision making does not ensure that it is providing leadership, guidance, and direction. For example, as pointed out on page 6, the chief of C³ has stated that he has not had sufficient authority to provide agencywide IRM leadership. Further, as we discuss on pages 5 and 6, top management has not clearly articulated how the organization will respond to current or future information requirements and uses of information technology.

We also believe that the individual efforts cited by the Coast Guard, such as the placement of standard workstations aboard vessels and shore units, or emphasis on source-data automation, do not represent a clear, comprehensive vision of how the agency can benefit from information technology. As discussed on pages 6 and 7, a strategic IRM plan would provide the mechanism to coordinate automated systems efforts such as these, and could be used by top management to articulate its vision to the organization. Because of this absence of a strategic IRM planning process and the unclear role and authority of the senior IRM official, we find the Coast Guard is lacking top-management leadership, guidance, and direction in managing information resources.

3. The Coast Guard takes exception to the assertion that its IRM focus is on technology-related solutions without an assessment of information needs. The Coast Guard cites several systems that have pursued the requirements analysis process as examples of an ongoing assessment of information needs, and sees this assessment as part of its modernization program. The Coast Guard also implies that because the systems we reviewed were in an evolutionary stage of development, adequate documentation appropriate to the current and planned stages of development was not available.

We disagree. As we discuss on pages 7 and 9, the absence of an agencywide IRM plan and an information architecture that concentrates on technology solutions, indicate that the Coast Guard is not paying sufficient attention to the organization's overall information needs. While some systems may have defined individual program needs, there has

been little assessment of the advantages and opportunities that would be created by addressing information needs that cross organizational boundaries. With regard to systems being in an evolutionary stage of development, half of the systems we reviewed had been in development for over 2 years, as illustrated on page 21.

4. The Coast Guard agrees with the need to develop a formal strategic IRM plan, and intends to promulgate additional policies, standards, and procedures. However, the Coast Guard also believes that in many cases the underlying objectives of formal plans, policies, and standards have already been successfully achieved through strict application of existing Coast Guard, Transportation, and General Service Administration (GSA) policies, standards, and procedures.

We agree that the Coast Guard needs to develop a strategic IRM plan and comprehensive policies, standards, and procedures. We do not agree that the Coast Guard has achieved the objectives that these mechanisms provide. As discussed on page 6, a strategic IRM plan provides the mechanism to set and evaluate priorities, and specifies how an agency's information technology will support its mission. During our review, we did not find evidence of any existing Coast Guard, Transportation, or GSA plan that is currently being used by the Coast Guard to accomplish this objective.

Further, the Coast Guard has not strictly applied existing policies, standards, and procedures. As we discuss on page 9, some project managers are cognizant of governmentwide standards and apply them to their system development efforts, while others rely on the C³ office to provide them what they need. Overall, we found that policies, standards, and procedures have been informally disseminated and disparately applied, with only informal oversight by the C³ office once projects have been initially funded.

5. The Coast Guard agreed that its current technology architecture may not fully address the mission objectives of current and future Coast Guard systems. However, it believes that this architecture is a significant starting point. The Coast Guard also stated that it is continuing to develop the architecture and improving the system-planning process.

We agree that the architecture is a good starting point. Nonetheless, as discussed on page 9, we believe that the formulation of the architecture suffers from the lack of guidance that an IRM plan and policies would provide. For example, it is not clear that the completed components of

the technology architecture fully address mission objectives of current and future systems, and the manner in which they will be employed. In addition, the Coast Guard has not set up a process for testing, implementing, or enforcing the architecture.

6. The Coast Guard recognizes that it has reached a critical phase in adapting IRM technology to better accomplish its organizational objectives. The Coast Guard believes that past efforts have resulted in significant accomplishments, that many of the difficulties pointed out in the report are well-known, and these difficulties constitute the reason for the current modernization effort.

We agree that the Coast Guard has reached a critical stage in adapting IRM technology to better accomplish its objectives. As discussed on page 4, we recognize that the Coast Guard has spent over a half-billion dollars on the acquisition and management of its information systems, and is aware of problems with its existing information systems. We believe, however, that the common problems that have affected existing Coast Guard systems point to an agencywide problem that the Coast Guard is not addressing. Until the Coast Guard fully addresses the recommendations made in this report, we believe investments made in the agency's information system infrastructure will run the risk of not meeting the agency's needs.

7. Current corrective actions cited by the Coast Guard appear to address our recommendation on the need for an IRM plan and IRM planning processes, but only partially address the other recommendations. The Coast Guard stated that it has started a program to provide top management with education on the strategic opportunities provided by information technology. However, the Coast Guard did not address (1) how top management will become more involved in the IRM decision-making process, or (2) the need to clarify the role of the designated senior IRM official.

The Coast Guard also notes that it is implementing Department of Defense standards for systems development and FIPS Pub 156[1] to strengthen policies and procedures used for the evaluation, development, and integration of information systems. The establishment of system development standards and a standard information resources

---

[1] Federal Information Processing Standard Publication 156, Guidelines for developing an Information Resources Dictionary System, National Institute of Standards and Technology, Apr. 5, 1989.

dictionary are positive steps toward developing comprehensive IRM policies, standards, and procedures to guide the implementation of information technology. The Coast Guard also needs to consider including the FIPS Pub standard as part of its overall information architecture.

Major Contributors to This Report

Information Management and Technology Division, Washington, D.C.

David G. Gill, Assistant Director
David L. McClure, Assignment Manager
Heidi L. Alves, Evaluator-in-Charge
Ruth Baskerville, Evaluator
Mary T. Marshall, Reports Analyst

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.