United States General Accounting Office

GAO

Testimony

For release on
Delivery
Expected at
10:00 a.m. EDT
Tuesday
April 24, 1990

Strategic Focus Needed to Improve the Coast Guard's Information Resources Management

Statement of
JayEtta Z. Hecker, Director
Information Management and Technology Division

Before the
Subcommittee on Coast Guard and Navigation
Committee on Merchant Marine and Fisheries
House of Representatives

G48327 / 141190

Mr. Chairman and Members of the Subcommittee:

I appreciate this opportunity to testify on the Coast Guard's management of its information resources. At the request of the Chairman of the House Merchant Marine and Fisheries Committee, we reviewed the general decision-making framework that the Coast Guard uses to plan, approve, and develop information technology projects to meet current and future mission needs. We are issuing a report to the Chairman today that provides further details of this work. As part of that request, we also submitted questions and information on systems development issues regarding specific systems for the Committee's use in reviewing the Coast Guard's fiscal year 1991 budget request.

As the Subcommittee is aware, information and information technology are powerful, strategic resources vital to the Coast Guard's ability to meet its responsibilities. Unfortunately, in many cases information is not collected, readily available, or easily transferable among Coast Guard units. GAO has reported to the Congress on how a lack of information has negatively affected both Coast Guard program operations and program management. For example, GAO recently testified that the Coast Guard's oil spill contingency plans in New York and Philadelphia did not contain specific information on how spills of various sizes would be handled with available resources. In the Exxon Valdez incident, the lack of such information contributed to the Coast Guard's inability to respond effectively. During our own review, we noted that the Coast Guard's law enforcement units lack timely access to information necessary to make tactical decisions supporting drug interdiction and vessel inspection boardings.

These examples highlight problems with the Coast Guard's use of information to support its missions and provide the backdrop against which we conducted our review. Today, I would like to focus on three areas: (1) information systems problems and current corrective actions, (2) the underlying causes contributing to the Coast Guard's information problems, and (3) steps we believe the Coast Guard should take to address its information resources management deficiencies.

INFORMATION SYSTEM PROBLEMS AND CURRENT CORRECTIVE ACTIONS

Mr. Chairman, in the past 6 years the Coast Guard has spent over half a billion dollars developing and operating its information systems. Yet, despite this investment, systems supporting critical Coast Guard missions cannot provide the information needed to effectively perform program operations. The Coast Guard has attempted to correct these problems by replacing or upgrading technical system components, but has not paid enough attention to an equally important area--the organization's overall information needs and information system requirements.

I would now like to direct your attention to the chart before you. (See attachment 1.) The chart shows several common problems that we identified with important existing information systems. As you can see, all five of the systems are affected by limited data query capabilities, which restrict users' ability to obtain information in a quick, easy fashion. Each system also has data integrity problems, making some information inaccurate and incomplete. System responsiveness and reliability problems have also interfered with users' ability to obtain information from four of the systems because response times are slow, computers are down, or data are not current. Further, some of the systems suffer from highly inefficient information transfer processes, such as field offices mailing their reports to headquarters where they are re-keyed into another system. These problems highlight the difficulties the Coast Guard is encountering in obtaining, using, and sharing high-quality information in a timely manner to effectively support critical missions in law enforcement, search and rescue, and marine environmental safety.

The Coast Guard is taking steps to address many of these shortcomings. Over the next 5 years, the agency plans to spend millions of dollars on computer hardware and software to modernize its information systems. The Coast Guard is also in the process of implementing an information technology architecture that will set up a standardized framework governing the deployment and use of its information technology.

While these positive steps may overcome many existing problems caused by technological obsolescence and inflexibility, we are concerned that they are being done without a critical reassessment of how the Coast Guard can more strategically use the power of information technology. Rather than using the power of information technology to transform and improve existing ways of conducting its business, the Coast Guard has developed most of its information systems to automate existing manual recordkeeping and reporting processes. Thus, despite improved office automation, neither the technology used nor the information generated has adequately supported Coast Guard operations. A strategic rethinking of its use of information technology is not accompanying or preceding the Coast Guard's computer modernization efforts. Without this rethinking, the modernization could become consumed with a project-by-project fix of existing systems problems without considering future as well as current agencywide information needs. By not addressing this concern, the Coast Guard passes on a key opportunity to better define its information systems needs and risks that its systems modernization investment will fail to meet its future information requirements.

UNDERLYING CAUSES CONTRIBUTING TO THE COAST GUARD'S INFORMATION PROBLEMS

Mr. Chairman, information resources management goes beyond determining and acquiring a configuration of computer hardware and software. Federal agencies must decide what information is essential to meet their responsibilities and how to effectively manage this information as a valuable organizational asset. At a recent GAO symposium, "Meeting the Government's Technology Challenge," leaders from industry, the Congress, and the executive agencies agreed that the keys to effective acquisition and management of information technology emphasize committed leadership, vision, and a concrete plan outlining how technology can be used to serve an agency's objectives.

The Coast Guard's approach to its modernization program only addresses the readily apparent causes of systems problems--existing hardware and software limitations. We believe three underlying and interrelated problems contribute to the Coast Guard's information problems: (1) a lack of information resources management leadership, (2) a lack of a strategic information resources plan, and (3) the absence of comprehensive information resources management policies and procedures. Until these problems are resolved, the Coast Guard runs the risk that its systems will be a loose collection of unrelated projects unable to meet agencywide information needs. Let me briefly discuss each of these problems in turn.

First, top-level Coast Guard leaders have not articulated how the organization will respond to current or future information requirements and uses of information technology. Although top management is involved in the Coast Guard's budget and planning process, this does not ensure that it is providing information resources management leadership, guidance, and direction. In fact, the Coast Guard's designated senior information resources management official has reported to the Chief of Staff that his designation is a classic case of responsibility without authority. The lack of clear support and direction from top management clouds an understanding of the role and authority of the senior information resources management official within the Coast Guard. This lack of support and authority limits his ability to provide agencywide IRM leadership, including integrating information projects that are logically related and which could more efficiently serve cross-functional information needs. Clearly, the absence of top leadership involvement generates a reactive rather than proactive environment, jeopardizing the success of the Coast Guard's technology initiatives.

Second, the Coast Guard does not have a strategic information resources management plan to set and evaluate priorities and to ensure that ongoing and proposed systems development projects logically support agency missions and goals. Instead, the Coast Guard uses its budget, planning, and review process to scrutinize and rank ADP procurements. This results in systems funding decisions based largely on individual Coast Guard office needs instead of on a comprehensive, coordinated, and agencywide perspective on information needs.

Third, the Coast Guard has not developed comprehensive policies, standards, and procedures for the management of its information resources. Policies, standards, and procedures add stability to an information resources management program, including system development efforts and would ensure that development projects will meet the Coast Guard's needs. Policies ensure that agencywide initiatives, such as information resource management control, review, and approval, are effectively implemented throughout the agency. System development standards and procedures provide guidelines for individual development projects. We found distinct differences in how standards, policies, and procedures were being applied to systems development projects. To further complicate this matter, no formal oversight by the senior information resources management official is exercised once projects are funded. Also, the Coast Guard's formulation of an information technology architecture suffers from a lack of guidance that information resources management policies could provide. By the Coast Guard's own admission, it has not set up a process to adequately test and implement its information technology architecture.

SUGGESTIONS FOR CHANGE

Information and the power of information technology are strategic assets to all organizations and are essential components of operational capabilities. Given that federal budget resources are scarce, it is increasingly vital that agencies make the most effective use of their investments in information technology. The information resources management decisions the Coast Guard makes today will affect its operations for years to come, as most of the new systems it is putting in place will not be fully operational until the mid 1990s and will continue to serve the Coast Guard into the 21st century. The Coast Guard needs committed leadership, strategic agencywide planning, and policies and procedures to guide effective implementation of systems once information resources management decisions have been reached.

However, our work at the Coast Guard shows that these essential elements are missing, putting information management and technology initiatives at a greater risk of not meeting agency needs. Our report contains recommendations to the Secretary of Transportation, noting that he should direct the Commandant to take the following steps to resolve the Coast Guard's information resources management problems: (1) clarify the role and authority of the Coast Guard's senior IRM official, (2) construct a strategic IRM plan that clearly states the agency's needs and the way information technology can serve these needs, and (3) implement comprehensive policies, standards, and procedures to guide information projects.

In commenting on our draft report, the Department of Transportation agreed with our findings and recommendations, specifically recognizing the need for improvement in the IRM strategic planning process. In its response, the Coast Guard stated that it would be taking steps to address our recommendations on strategic IRM planning and the need for additional IRM policies, standards, and procedures. However, 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 level management will be involved in managing information resources.

We believe that by not acting on all our recommendations, the Coast Guard risks that the information systems it develops will fail to meet its current and future needs. With this Subcommittee's attention and support during the leadership transition at the Coast Guard, we believe the Coast Guard can improve the contribution of information technology toward achieving its complex and diverse mission.

Mr. Chairman, this concludes my statement. Thank you again for this opportunity to present our views to the Subcommittee. I will be happy to answer any questions that you or other members of the Subcommittee may have about our work.

Common Problems With Existing Coast Guard Information Systems

SYSTEM	Limited Query Ability	Data Integrity Problems	Responsiveness & Reliability Problems	Data Transfer Difficulty
Aircraft Repair and Supply Center System[a]	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
Personnel Assignment Management Information System (PAMIS)	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).