United States General Accounting Office

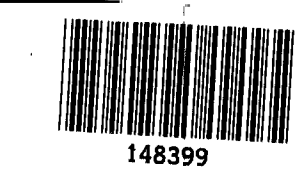
GAO

Report to the Chairman, Subcommittee on Research and Development, Committee on Armed Services, House of Representatives

December 1992

MISSION-CRITICAL SYSTEMS

Defense Attempting to Address Major Software Challenges



GAO/IMTEC-93-13

GAO

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

Information Management and
Technology Division

B-251388

December 24, 1992

The Honorable Ronald V. Dellums
Chairman, Subcommittee on
Research and Development
Committee on Armed Services
House of Representatives

Dear Mr. Chairman:

Billions of dollars in current and future Defense weapons and command, control, communications, and intelligence (C^3I) systems depend on high-performance, correctly functioning, real-time computer systems capable of withstanding severe stresses without failing. This report responds to your March 1992 request that we provide you with an overview of our work on mission-critical systems. Specifically, you asked that we identify (1) common software development problems affecting these systems, (2) what factors contribute to their continuation, and (3) what actions Defense is taking to address software development problems. Appendix I details our objectives, scope, and methodology.

Results in Brief

Defense's mission-critical systems continue to have significant software development problems. Numerous GAO reports and Defense studies have identified many problems, including a lack of management attention, ill-defined system requirements, and inadequate testing. The highly complex nature of mission-critical systems and the millions of lines of software required to support them contribute to the continuation of serious software development problems. Defense is attempting to address these problems primarily through two major efforts—the software action plan working group and the Corporate Information Management initiative. Whether these two initiatives will solve Defense's formidable software problems is uncertain; there are no easy answers.

Background

In 1982 the Warner Amendment (10 U.S.C. 2315) distinguished Defense's mission-critical systems from business-oriented automated information systems. It defined mission-critical systems as those that are (1) intelligence- and cryptologic-related, (2) command and control of military forces-related, (3) integral to a weapons system, or (4) critical to fulfilling military or intelligence missions that are not used for routine administrative and business applications. The mission-critical systems that

we reviewed were either C³I or embedded weapons systems. C³I systems are intended to provide a commander with hardware and software need to collect and assimilate pertinent information from voluminous amount of data and to accomplish effective decisionmaking in a short time fram Embedded computer systems include any computer hardware or softwa that is physically part of and necessary for a weapons system to perform its full mission. New major weapons systems currently being developed depend on the successful development of millions of lines of software. However, to date, development of large amounts of software supporting complex systems has been riddled with significant problems.

Software Problems Have Continued to Hinder Successful System Development

Over the past several years, numerous GAO reports and Defense studies have identified chronic software-related management and technical shortfalls plaguing mission-critical systems. Generally, GAO reports have been more system-specific, while Defense studies have covered broader underlying issues such as problems stemming from the major acquisitio process.

GAO Reports Cite Significant System Software Problems

Over the last several years, we have reported on many software development problems for weapons and other mission-critical systems. Many of the problems fall into three general and overlapping categories: (1) management, (2) requirements definition, and (3) testing.

We categorized management problems as those that managers had direc control over. For example, in some cases, managers allowed acquisition to proceed prematurely, i.e., before assuring that the software was adequate, or after significant software problems had been identified. In other cases, managers did not have sound approaches to software development, nor did they adequately oversee development efforts. Requirements definition, the logical depiction of what a system is supposed to do both now and in the future, has been a recurring proble for Defense. Problems included ill-defined requirements, changing requirements, and systems that were not flexible enough to adapt to changing requirements. Finally, approaches to testing were often flawed Examples included using inaccurate models to test against and omitting system-level integration testing.

These management, requirements definition, and testing problems contribute to significant schedule delays, cost increases, and performan shortfalls. A case in point is the Cheyenne Mountain Upgrade (CMU). In

June 1992 we reported that this system will be delivered 8 years late, cost at least $600 million more than planned, and have less capability than originally planned.[1]

Appendix II summarizes our more recent reports on software development problems with major Air Force, Navy, Army, and Strategic Defense Initiative Organization systems. Table 1 provides a system reference denoting the system acronym, system name, and page reference to appendix II. Table 2 lists the system software development problems identified during our reviews.

Table 1: System Reference

Acronym	System Name	Page
CMU	Cheyenne Mountain Upgrade	14
CSSR	Communications System Segment Replacement	16
SPADOC	Space Defense Operations Center	16
SCIS	Survivable Communications Integration System	17
Q-93	AN/FQ-93 computer for the North American Aerospace Defense Command	17
CCS	Command and Control Segment for satellite control	18
C-17	C-17 transport aircraft	19
LAMPS	Light Airborne Multipurpose System Mk I helicopter	20
P-3/ Update IV	P-3 Submarine Patrol Aircraft/Avionics Update IV	20
F-14D	F-14D "Tomcat" fighter aircraft	21
BSY-2	AN/BSY-2 combat system for SSN-21 Seawolf submarine	22
ATCCS	Army Tactical Command and Control System	23
FDDM	Fire Direction Data Manager for the Army's Multiple Launch Rocket System	23
Patriot	Patriot surface-to-air missile system	24
SDI	Strategic Defense Initiative	25

[1]Attack Warning: Lack of System Architecture Contributes to Major Development Problems (GAO/IMTEC-92-52, June 11, 1992).

Table 2: Software Development Problems and Systems Reported on by GAO

Categories of Problems	Systems
Management	
Lack of management attention/ oversight	CMU, SPADOC, C-17, LAMPS, BSY-2, ATCCS, SDI
Lack of adequate software management concepts, methods, practices	CMU, SPADOC, C-17, F-14D, BS' FDDM
Lack of adequate planning	CMU, Q-93, C-17, ATCCS
Development proceeded despite serious problems	CSSR, SPADOC, C-17, LAMPS, P3/ Update IV, F-14D, BSY-2
Requirements Definition	
Lack of well-defined requirements	CMU, CSSR, SPADOC, SCIS, CC C-17, P3/Update IV, BSY-2, ATCC FDDM
Requirements change to meet new missions	CMU, Q-93, CCS, SDI
Lack of overall system perspective	CMU, CSSR, Q-93, ATCCS, SDI
System not readily able to adapt to change	CMU, Q-93, CCS, SDI
Software products cannot/may not meet security requirements	CMU, SPADOC, SDI
Testing	
Lack of adequate testing methods and approaches	CCS, C-17, LAMPS, P-3/ Update F-14D, BSY-2, Patriot, SDI
Lack of adequate system-level integration testing	C-17, P-3/Update IV, ATCCS, F-1 SDI

Defense Studies Also Identify Numerous Software Issues

Over the past decade, Defense studies have identified a wide variety of software issues, including those reported on by GAO. Broader in scope, these studies address issues ranging from shortfalls in existing software acquisition policies and management to problems with the delivered software and shortages of qualified personnel.[2] For example, policy and management problems included the lack of a defined overall software management, development, and requirements policy; uncoordinated and conflicting software policies; inadequate software management concept methods, and practices; and lack of clearly defined roles and responsibilities. Moreover, Defense studies identified many problems associated with the entire software acquisition process, including flawe requirements setting and inadequate development methodologies.

In addition to identifying software-related problems, Defense studies als attempt to address causes. For example, several studies stated that

[2]Studies include the 1987 Report of the Defense Science Board Task Force on Military Software, 19 Report of the Workshop on Military Software, and the 1990 draft Software Master Plan.

building large, complex systems all at once made requirements definition and system management difficult. They stated that current system acquisition policies should be changed to allow for more incremental or evolutionary development. Such development allows the system to be built in phases rather than all at once. That is, initial requirements are identified first and are used to build a first phase with initial capabilities. Subsequent phases add more capabilities until the system is complete.

Inherent Mission-critical System Characteristics Contribute to Development Problems

Given the number of reports and studies highlighting software development problems and identifying courses of action, why is it so difficult to correct these problems? One key reason is that most mission-critical systems require millions of lines of software and are by nature highly complex. How to produce high quality software for such systems is poorly understood. Unlike most hardware products, it is difficult to accurately measure software's essential characteristics: correctness, robustness, performance, security, and integrity. Further, developers find it difficult to accurately measure the progress of developing software products. These problems increase with increasing system complexity.

Complexity arises from the missions that these systems perform and the environment in which they operate. For example, to perform such functions as integrating multiple-sensor data or defending against a ballistic missile attack, mission-critical systems generally must incorporate state-of-the-art technologies. These systems must operate in a geographically distributed, real-time environment, interoperate with other complex systems, have highly reliable software, and adapt to change. Further, these C^3I and embedded weapons systems must continue to operate during wartime despite the enemy's attempts to destroy or disrupt them.

In spite of the widespread use of mission-critical systems, development attempts are currently fraught with serious limitations. For example, in February 1992, we reported that many of the technologies—real-time, distributed, computing supported by highly reliable software—needed to deploy a ballistic missile defense system were immature at best.[3]

[3]Strategic Defense Initiative: Changing Design and Technical Uncertainties Create Significant Risk (GAO/IMTEC-92-18, Feb. 19, 1992).

Defense Attempting to Address Software Challenges

Over the years, Defense has had many initiatives addressing software issues; recently, two major efforts have emerged. The Undersecretary for Acquisition through the Director of Defense Research and Engineering (DDR&E) is spearheading the software action plan working group, and the Assistant Secretary for C^3I is leading the Corporate Information Management (CIM) initiative.

The Software Action Plan Working Group: DDR&E's Attempt

In June 1991, recognizing software's criticality to future Defense effectiveness and its increasing share of weapons system costs, the Secretary of Defense instituted a software action plan working group to b led by DDR&E. Its intent is to develop and implement integrated management and technology plans to ensure more cost-effective softwar support for mission-critical systems.

The software action plan working group is addressing management issue without a formal written plan to guide their activities. Instead, the workir group has identified and begun to implement a number of tasks. These tasks include the following: developing standards and practices, identifying Defense oversight software expert reviewers, certifying software personnel, and improving software reuse and software acquisition. The intent over the next few months is to document what progress has been made in each of the task areas and leverage additional work appropriately.

In December 1991 DDR&E prepared a draft technology plan known as the Software Technology Strategy, which has been reviewed by industry, academia, and the Department itself.[4] The technology plan is intended to assess Defense's software needs for mission-critical systems and to defin technology investments over the next 15 years. It has identified five majo strategic themes: reusing software and advancing programming techniques, reengineering and improving software maintenance, integrating technical and management software aspects, leveraging commercial technology, and integrating artificial intelligence and softwai engineering technology. Six technology areas and their respective milestones are identified and include software and systems engineering, human-computer interaction, artificial intelligence, parallel and heterogeneous distributed systems, real-time fault-tolerant software, and high-assurance software. DDR&E is currently developing an implementatio plan.

[4]The Software Technology Strategy was published in draft. It will be periodically updated as part of a broader effort known as the DOD Key Technologies Plan.

CIM Programs: C^{3}I's Attempt

Defense initiated CIM primarily to improve business operations in functional areas such as payroll, personnel, and logistics, and to eliminate and reduce redundant automated information systems supporting these functions. In 1990 CIM's purview expanded to include some mission-critical C^{3}I systems; Defense is currently determining how and which systems will be included under CIM.

Through CIM, Defense plans to develop a technology infrastructure based on Departmentwide standards. The move to this technology infrastructure, according to Defense documentation, requires changes in the way Defense handles the building blocks of information technology: the data, the computers, the programs, and their operations. Three programs—data administration, software reuse, and Integrated Computer-aided Software Engineering (ICASE)—highlight CIM's attempt to address the state-of-the-practice of software technologies.

The data administration program is an attempt to provide consistent, unambiguous, and easily accessible data Defensewide. The program is attempting to minimize the cost and time required to make systems and their data compatible. A simple example to illustrate the importance of common data names is an organization's use of social security numbers to track personnel. One component of an organization could call it SSN while another component could call it SocNum. Having different names that identify social security numbers makes it more difficult for these components to share information; to facilitate data sharing, the data element name should be identical. Hence, by standardizing and registering these data elements and their names, Defense will facilitate data sharing.

The software reuse initiative is a joint DDR&E and C^{3}I attempt to implement a broad, consistent, Departmentwide reuse strategy. Associated policies, practices, approaches, and programs are attempting to achieve significant levels of software reuse to permit sharing where appropriate and to obtain maximum benefits from reusing existing software rather than developing it from scratch.

The ICASE program is intended to provide a standard software engineering environment for developing and maintaining automated information systems. The acquisition will include process and data modeling tools, a full range of software life-cycle development tools, and an information repository for integrating data used among the tools. The ICASE program standard software engineering environment will be required for maintaining all CIM systems.

Conclusions

As systems become increasingly complex, successful software development becomes increasingly difficult. Most major system developments are fraught with cost, schedule, and performance shortfall We have repeatedly reported on costs rising by millions of dollars, schedule delays of not months but years, and multibillion-dollar systems that don't perform as envisioned. Defense also recognizes this situation. Over the years, it has initiated many studies and initiatives that have identified software problems and attempted to address them.

Why do serious software shortfalls continue? They continue because the are no easy answers. The understanding of software as a product and of software development as a process is not keeping pace with the growing complexity and software dependence of existing and emerging mission-critical systems. Defense is, however, attempting to address this dilemma through its two major initiatives. Whether these are the right initiatives or whether they are able to solve or even address Defense's formidable software challenges is yet to be determined.

We conducted our review from April 1992 through December 1992, in accordance with generally accepted government auditing standards. As requested, we did not provide a draft of this report to the Department of Defense for its review and comment. Instead, we discussed the report's facts with officials, including the special assistant to DDR&E, the acting assistant deputy director of C^{3}I's Information Technology Division, and service representatives, who generally agreed with the facts as presented We have incorporated their views in the report as appropriate.

We plan no further distribution of this report until 30 days from the date of this letter. We will then send copies to the Secretary of Defense and other interested parties. Copies will also be made available to others upon request. Should you have any questions concerning this report, please contact me at (202) 512-6240. Major contributors to this report are listed in appendix III.

Sincerely yours,

Samuel W. Bowlin
Director, Defense and Security
Information Systems

Contents

Abbreviations

ATCCS	Army Tactical Command and Control System
BM/C^3	Battle Mangement/Command, Control, and Communications
C^{3}I	Command, Control, Communications and Intelligence
CCPDSR	Command Center Processing Display System Replacement
CCS	Command and Control Segment
CIM	Corporate Information Management
CMU	Cheyenne Mountain Upgrade
CSSR	Communications System Segment Replacement
DDR&E	Director of Defense Research and Engineering
DOD	Department of Defense
FDDM	Fire Direction Data Manager
GAO	General Accounting Office
GPALS	Global Protection Against Limited Strikes
ICASE	Integrated Computer-aided Software Engineering
IMTEC	Information Management and Technology Division
LAMPS	Light Airborne Multipurpose System
NORAD	North American Aerospace Defense Command
SCIS	Survivable Communications Integration System
SDI	Strategic Defense Initiative
SDIO	Strategic Defense Initiative Organization
SPADOC	Space Defense Operations Center
SSN	social security number

Objectives, Scope, and Methodology

In March 1992 the Subcommittee on Research and Development, House Committee on Armed Services, requested that we provide an overview of our work on mission-critical systems, including computer systems embedded in Defense weapons. The Subcommittee asked us to identify (1) common software development problems affecting these systems, (2) what factors contribute to their continuation, and (3) what actions Defense is taking to address them. Our review is part of the House Armed Services Committee's overall request to review computer systems that ar embedded in Defense weapons systems. Because our study is based on selected reports, it is not intended to be a statistical study; it is only intended to provide a snapshot of selected problems and Defense's major attempts to address them.

To accomplish our first objective, we analyzed over 20 GAO case studies involving software or software-related problems in Air Force, Navy, Army and Strategic Defense Initiative Organization systems. We identified common problems and categorized them accordingly. We corroborated our analysis by reviewing key Defense studies, which identified many of the same problems. These studies include the Report of the Defense Science Board Task Force on Military Software and the preliminary draft of the Software Master Plan, which contained comprehensive summary information on Defense studies, common problems, and courses of actior We also discussed our identified problems and categories with various Defense software experts, including officials from DDR&E, C^3I, and the services.

To accomplish our second objective, we reviewed additional documentation discussing the inherent characteristics of mission-critical systems. We reviewed such documents as the DOD Key Technologies Plan and the Institute of Defense Analyses' studies, such as the Assessments o Selected Real-Time Computing Technologies.

Our third objective was met by (1) reviewing the Software Master Plan's summary of initiatives; (2) reviewing other Defense documents, including the software action plan briefing, the Software Technology Strategy, and the Status of the Department of Defense Corporate Information Management (CIM) Initiative; and (3) discussing initiatives with DDR&E and CIM officials.

We performed our work at DDR&E and C^3I offices at the Pentagon; the Defense Advanced Research Projects Agency, Arlington, Va.; the Defense

Systems Management College, Ft. Belvoir, Va.; and the Institute for Defense Analyses, Alexandria, Va.

Defense Systems and Related GAO Reports

Air Force Systems

Cheyenne Mountain Upgrade (CMU)

CMU is the Air Force's attempt to modernize the Integrated Tactical Warning and Attack Assessment System, which is used to support information processing needs for the North American Aerospace Defense Command (NORAD). It includes five subsystems: the Command Center Processing Display System Replacement (CCPDSR), the Communications System Segment Replacement (CSSR), Granite Sentry, Space Defense Operations Center (SPADOC), and the Survivable Communications Integration System (SCIS).

Attack Warning: Lack of System Architecture Contributes to Major Development Problems (GAO/IMTEC-92-52, June 11, 1992)

Findings:

(1) The Air Force is developing CMU as five individual subsystems without an overall system architecture to tie the five subsystems together so they can function as an integrated unit.

(2) Until an overall CMU system architecture is defined, the Air Force will encounter serious development and integration problems and cost increases, and will have a system that is not readily evolvable to adapt to mission changes.

(3) No systemwide security architecture exists, as each contractor selected hardware and software on the basis of its interpretation of what i needed to provide for a secure system.

(4) Because of its focus on cost and schedule, the Air Force is developing a system with less capability than originally planned and has deferred some requirements until after the delivery date.

Attack Warning: Better Management Required to Resolve NORAD Integration Deficiencies (GAO/IMTEC-89-26, July 7, 1989)

Findings:

(1) The Air Force's large, complex integration management structure

fragmented management functions, responsibility, and accountability among numerous commands.

(2) The Air Force's cumbersome and lengthy resolution process has not been able to resolve such critical integration problems as the use of different communications standards and attack scenarios among CMU subsystems.

(3) Unresolved problems could disrupt the Air Force's ability to effectively integrate the modernized subsystems into CMU.

(4) Subsystem development and integration occurred amid constant management change, with frequent turnover among program managers, commanders, principal deputies, and command managers.

(5) The modernization programs established a pattern of deferring, rather than solving, the system development problems they identified.

Attack Warning: Defense Acquisition Board Should Address NORAD's Computer Deficiencies (GAO/IMTEC-89-74, Sept. 13, 1989)

Findings:

(1) The Air Force identified 29 unresolved critical deficiencies in the 5 modernization programs.

(2) Work began to resolve critical CSSR program problems involving uniform wiring standards, cabling congestion, and standardized message formats, but did not address other critical problems involving standard communication protocols or inconsistent message-loading assumptions, although the Air Force recognized that the effectiveness of its other modernization programs relied on CSSR.

(3) The Air Force accepted CSSR hardware that did not conform to 12 system specifications and planned to accept the hardware without completing tests and with incomplete software.

(4) The Air Force continued interim CSSR upgrades, but did not perform a recommended cost-benefit analysis to determine the most efficient and effective means for satisfying communications processing requirements.

Communications System Segment Replacement (CSSR)

The Air Force's CSSR program is an effort to acquire a replacement system for the communications portion of CMU.

Attack Warning: NORAD's Communications System Segment Replacement Program Should Be Reassessed (GAO/IMTEC-89-1, Nov. 30, 1988)

Findings:

(1) The Air Force planned to accept CSSR's Block I unit although it had critical software design deficiencies, did not meet restart requirements, and contained wiring standard and equipment incompatibility that precluded its installation.

(2) The Air Force has deferred fixing identified CSSR problems such as unreliable message processing, inadequate computer system availability, software and hardware maintenance, and expansion limitations.

(3) Without a common message set, consistent message-load requirements, and a standardized communications protocol, CSSR cannot be fully operational.

Space Defense Operations Center (SPADOC)

SPADOC is the Air Force's attempt to modernize the United States Space Command's space surveillance and attack assessment subsystem. SPADOC is intended to be a data processing and communications center that can monitor and maintain orbit information on up to 10,000 man-made object in space, provide timely warning of any threat or attack, and protect satellites by identifying the need for satellite maneuvers.

Space Defense: Management and Technical Problems Delay Operations Center Acquisition (GAO/IMTEC-89-18, Apr. 20, 1989)

Findings:

(1) The Air Force invested over $235 million in SPADOC, which was, at the time, more than 4 years behind schedule and did not meet its required operational capability.

(2) The Air Force continued to press forward with the program despite contractor warnings that it would be difficult to meet requirements, and with the knowledge that the contractor testing model was deficient.

(3) The Air Force consistently deferred resolution of problems involving controlled mode security, software development, performance prediction model validity, and design integrity to later development phases.

(4) The Air Force knew that achieving some Block A requirements would be risky and needed close management oversight. However, the Air Force accepted Block A, which did not meet most of its requirements and was not operational.

Survivable Communications Integration System (SCIS)

As part of the CMU program, SCIS is planned to be an automated communications system that will process and simultaneously send missile attack warning messages across different media to national decisionmakers.

Attack Warning: Status of the Survivable Communications Integration System (GAO/IMTEC-92-61BR, July 9, 1992)

Findings:

(1) The program had been delayed 3 years because the hardware had to be replaced by more powerful computers and the missile warning message requirements needed to be redefined.

(2) Air Force reductions in the number of communications media, from five to three, reduced SCIS survivability.

Q-93

The AN/FQ-93 is a NORAD computer that receives, processes, and correlates radar data from nine regional or sector operations control centers in Hawaii, Alaska, Canada, Iceland, and the continental United States.

Computer Technology: Air Attack Warning System Cannot Process All Radar Track Data (GAO/IMTEC-91-15, May 13, 1991)

Findings:

(1) The Air Force's Q-93 architecture had only limited expansion capabilities to accommodate changing processing work loads and requirements.

(2) Air Force studies identified serious problems with Q-93 memory available to process and store aircraft tracks generated from planned ra sources.

(3) The Air Force did not adequately analyze Q-93 capacity and performance capabilities or establish a formal capacity management an performance monitoring program.

(4) Defense did not manage the components of the atmospheric attack warning/attack assessment system from a system-level perspective.

(5) Although Defense spent almost $3 billion to acquire planned radar upgrades and additions for atmospheric attack warning/attack assessme and counter-narcotics missions, it did not resolve how the work load generated by those radars would be effectively processed and forwarde to decisionmakers.

Command and Control Segment (CCS)

The Air Force's new satellite control system, CCS, is designed to provide command and control instructions to support the launch and maintain t operation and position of on-orbit satellites that provide critical defense communications, navigation, surveillance, and weather services.

Military Space Operations: Satellite Control System Improved, But Serio Problems Remain (GAO/IMTEC-92-3, Dec. 27, 1991)

Findings:

(1) The Air Force may not meet the July 1993 operational deadline because of critical CCS operational deficiencies.

(2) New requirements, in part, contributed to incomplete software and insufficient capacity.

(3) The Air Force has not developed an adequate capacity and performance management program, defined work-load requirements, adequately tested CCS, or obtained adequate software documentation.

(4) If the Air Force does not resolve these problems, it will have to continue using its old system, the Current Data System, spending $30 million annually to maintain an outdated system.

Other Related Reports:

Military Space Operations: Shuttle and Satellite Computer Systems Do Not Meet Performance (GAO/IMTEC-88-7, Aug. 5, 1988)

Military Space Operations: Operational Problems Continue with the Satellite Control Computer System (GAO/IMTEC-89-56, Aug. 8, 1989)

Defense Acquisition: Air Force Prematurely Recommends ADP Acquisitions (GAO/IMTEC-90-7, Mar. 29, 1990)

C-17 Transport Aircraft

The C-17 is an Air Force transport aircraft that is designed to airlift large payloads and oversized cargoes onto small airfields.

Embedded Computer Systems: Significant Software Problems on C-17 Must Be Addressed (GAO/IMTEC-92-48, May 7, 1992)

Findings:

(1) At the start of the full-scale engineering development effort, the Air Force did not completely identify C-17 software development requirements or determine how difficult it would be to develop and integrate sophisticated software subsystems.

(2) The Air Force did not ensure that the contractor's software development and management capabilities were adequate, and underestimated software development risks.

(3) To meet the September 1991 first-flight schedule, the Air Force allowed the contractor to take shortcuts that have increased software development risks. For example, the contractor deleted some system-level integration testing prior to the first flight.

(4) When the developmental C-17 aircraft first flew, it contained only 66 percent of the newly developed software needed to make the aircraft avionics fully functional.

(5) Despite the contractor's lack of software experience, the C-17 contract gave the contractor total control over software development; limited the Air Force's access to software cost, schedule, and performance information; and restricted the Air Force from correcting critical software problems when they became evident.

(6) The Air Force has allowed the contractor to develop C-17 software i diverse assortment of languages, which may result in increased maintenance costs. Further, a lack of documentation may hinder the Ai Force from upgrading, testing, and maintaining C-17 computer systems.

Navy Systems

Light Airborne Multipurpose System (LAMPS)

The Navy's LAMPS Mk I is a ship-based helicopter that performs antisubmarine warfare (i.e., locates, identifies, follows, and engages ene submarines).

Embedded Computers: Navy Not Ready to Buy Avionics Computers for LAMPS Mk I Helicopters (GAO/IMTEC-90-54, May 31, 1990)

Findings:

(1) The Navy planned to decide on whether to buy upgraded avionics computer systems for $6.6 million before operationally testing the syste

(2) The planned upgraded system was significantly different from the already-approved computer system.

(3) Developmental testing revealed significant software problems and raised concerns about whether the Navy should proceed before the problems were corrected.

(4) Laboratory integration testing did not realistically simulate the environment in which the software would operate while actually trackir submarines.

(5) The Navy has not ensured compliance with operational testing requirements for the systems because of its belief that the system is a minor modification of an existing computer system.

P-3/Update IV

The acquisition for submarine patrol aircraft, designated the P-3/Update program, is an attempt to provide the Navy with the capability to locate, identify, and attack the expected threat of more quiet submarines.

Embedded Computers: Navy's Approach to Developing Patrol Aircraft Avionics System Too Risky (GAO/IMTEC-90-79, Sept. 28, 1990)

Findings:

(1) The Navy planned to buy 28 systems before it successfully completed all testing and failed to consider the costs of buying systems that may not work as intended and may require expensive modifications.

(2) The Update IV contractor was allowed to develop software before it completed subsystem specifications.

(3) The Navy had approved only 3 of 93 software specifications, and projected that it would not approve all specifications before it would begin buying the systems.

(4) The extent of integration testing had been reduced.

(5) The Navy planned to test one of the system's processors using a model that did not accurately represent its functionality and performance capability.

F-14D Fighter Aircraft

The Navy's F-14D "Tomcat" fighter is designed for missions involving air defense, fighter escort, and air-to-surface weapons delivery.

Embedded Computer Systems: F-14D Aircraft Software Is Not Reliable (GAO/IMTEC-92-21, Apr. 2, 1992)

Findings:

(1) The F-14D aircraft could not meet its intended mission due in part to software problems that prevented the aircraft from functioning properly, e.g., cockpit displays had gone blank and erroneous data were supplied to the mission computer.

(2) The Navy's software development testing approach and model were inadequate and increased the risk that more serious defects may still be unidentified.

(3) The Navy did not follow software development standards that recommend independent testing of a contractor's product before

acceptance, the use of detailed design specifications as criteria for testin and thorough testing of each function for compliance with design requirements.

(4) The Navy was correcting F-14D software problems. Before completin these efforts, the Navy planned to develop and add previously deferred software functions to the aircraft.

(5) The new software depended on the stability and reliability of the existing software; proceeding with previously deferred software function before ensuring that existing software functions were reliable will complicate and increase software problems.

BSY-2 Combat System

The BSY-2 is a combat system for the new SSN-21 Seawolf attack submarine. It is an advanced computer system designed to detect, classif track, and launch weapons at enemy subsurface, surface, and land target

Submarine Combat System: BSY-2 Development Risks Must Be Addresse and Production Schedule Reassessed (GAO/IMTEC-91-30, Aug. 22, 1991)

Findings:

(1) A 1-year delay in completing the critical design review further compressed the already tight development schedule.

(2) The Navy based system development and production decisions on incomplete test and evaluation results.

(3) Late government-witnessed testing left the Navy with limited time and flexibility to identify specific problems and bring them to the attention of the contractor without affecting system delivery.

(4) The Navy did not ensure that major software component retesting wa adequate to verify that other portions of such components were not adversely affected by software changes.

(5) The contractor experienced problems in meeting start-up requirement in using a new standard Navy signal processor, and preliminary estimates indicated that processing capacity may be inadequate.

Other Related Reports:

Submarine Combat System: Technical Challenges Confronting Navy's Seawolf AN/BSY-2 Development (GAO/IMTEC-89-35, Mar. 13, 1989)

Submarine Combat System: Status of Selected Technical Risks in the BSY-2 Development (GAO/IMTEC-91-46BR, May 24, 1991)

Submarine Technology: Transition Plans Needed to Realize Gains from DOD Advanced Research (GAO/IMTEC-90-21, Feb. 14, 1990)

Army Systems

Army Tactical Command and Control System (ATCCS)

ATCCS is the Army's attempt to integrate five command and control systems. It is designed to rapidly collect, process, analyze, display, coordinate, and exchange timely battlefield information to enhance commanders' decisionmaking processes.

Army Battlefield Automation: Oversight Needed to Assure Integrated System (GAO/IMTEC-90-78, July 24, 1990)

Findings:

(1) The Army did not fully define how the component systems would integrate into the overall ATCCS configuration.

(2) The Army needed to resolve over 40 technical problems that were important in developing and integrating the component systems into ATCCS.

(3) The Army did not analyze the communications work load to determine whether the communications systems for ATCCS would be adequately sized.

(4) No system-level oversight had occurred, and the Army was only in the process of establishing a system-level test and evaluation master plan.

Fire Direction Data Manager (FDDM)

FDDM is being developed to provide communications, data processing, and fire direction capabilities for a group of munitions fired from the Army's Multiple Launch Rocket System launcher.

Embedded Computer Systems: Software Development Problems Delay Deployment of the Army's Fire Direction Data Manager (GAO/IMTEC-92-32, May 11, 1992)

Findings:

(1) The Army's FDDM development effort encountered a number of software problems that must be corrected before the system can be deployed, e.g., the inability to keep its fire direction and data processing databases synchronized.

(2) The prime contractor's costs tripled from about $8 million to about $24.5 million, primarily due to added requirements.

(3) FDDM software development problems occurred primarily because the Army did not adequately define initial requirements for the system or promptly enforce Defense standards for software development.

(4) The contractor did not develop or use a detailed software developme plan as a guide to develop the software, and the contractor's initial communications testing was inadequate, causing software development delays because of problems that were not detected until later in the development process.

Patriot Missile System

The Patriot is an Army surface-to-air, mobile air defense missile system.

Patriot Missile Defense: Software Problem Led to System Failure at Dhahran, Saudi Arabia (GAO/IMTEC-92-26, Feb. 4, 1992)

Findings:

(1) The Patriot battery at Dhahran failed to track and intercept a Scud missile due to a software problem in the system's weapons control computer.

(2) The software problem caused an inaccurate tracking calculation, which became worse the longer the system operated.

(3) The Army had never used the Patriot to defend against tactical ballisti missiles and expected the Patriot to operate continuously for long period of time. It had not been tested for the long run times.

Multiservice Systems

Strategic Defense Initiative (SDI)

In 1983 SDI was begun with the purpose of researching the feasibility of developing a system to protect America against massive ballistic missile attacks from the Soviet Union. Over the past decade, SDI has undergone repeated changes in its objectives and system design. Previously known as Phase I, the current SDI system is intended to defend against a limited ballistic missile attack from any country and is known as Global Protection Against Limited Strikes (GPALS).

Strategic Defense System: Stable Design and Adequate Testing Must Precede Decision to Deploy (GAO/IMTEC-90-61, July 6, 1990)

Findings:

(1) The system would not be deployed unless the President certified to Congress that the system could maintain effectiveness during a war and fulfill its mission. The Strategic Defense Initiative Organization's (SDIO) goal was to decide to deploy Phase I by 1993.

(2) In January 1990 a new subsystem known as Brilliant Pebbles fundamentally changed the Phase I architecture. Consequently, the architecture would not be solidified until 1991, thus decreasing the level of system testing that can be performed by 1993.

(3) By 1993 SDIO will not have conducted integrated system-level tests designed to demonstrate that the entire Phase I system will work as planned.

(4) Some subsystem tests will be based on immature models.

(5) Major architectural decisions were made without formal Defense Acquisition Board review.

Strategic Defense Initiative: Changing Design and Technological Uncertainties Create Significant Risk (GAO/IMTEC-92-18, Feb. 19, 1992)

Findings:

(1) SDIO is continuing its efforts to design a ballistic missile defense system

now known as the Global Protection Against Limited Strikes (GPALS) system to address the change in program focus from deterrence to protection, but it has not solidified the GPALS architecture.

(2) Until SDIO solidifies the GPALS architecture, there is an increased risk that its subsystems will be incompatible.

(3) If SDIO includes integration capabilities for space-based interceptors into the missile defense system but never deploys them, it will incur unnecessary costs; but if SDIO does not include space-based interceptor capabilities in the missile defense system and the inclusion is later deem necessary, costly reengineering will be required.

(4) Resolving technical challenges in the GPALS subsystem—Battle Management/Command, Control, and Communications (BM/C^3)—is essential to GPALS development.

(5) BM/C^3 software may have to operate on parallel processors and will require a highly sophisticated software engineering and development environment that is not currently available.

(6) The GPALS software security requirements have not been defined.

Major Contributors to This Report

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

John B. Stephenson, Assistant Director
Sally M. Obenski, Evaluator-in-Charge
Paula Bridickas, Staff Evaluator

Ordering Information

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

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

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

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

Official Business
Penalty for Private Use $300

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100