United States General Accounting Office

GAO

Report to the Secretary of the Navy

June 1998

DEFENSE COMPUTERS

Year 2000 Computer Problems Put Navy Operations at Risk

GAO/AIMD-98-150

GAO

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

Accounting and Information
Management Division

B-279872

June 30, 1998

The Honorable John H. Dalton
The Secretary of the Navy

Dear Mr. Secretary:

This report presents the results of our review of the Navy's program for addressing its Year 2000 computer systems problem. The problem results from the inability of computer systems at the year 2000 to interpret the century correctly from a recorded or calculated date having only two digits to indicate the year. Time is running out to correct Navy systems that could malfunction or produce incorrect information when the year 2000 is encountered during automated data processing. The impact of these failures could be widespread, costly, and potentially debilitating to important Navy operations worldwide.

We performed this work as part of our review of the Department of Defense's (DOD) Year 2000 computer systems efforts for the Chairman, Senate Committee on Governmental Affairs; the Chairman and Ranking Minority Member of the Subcommittee on Government Management, Information and Technology, House Committee on Government Reform and Oversight; and the Honorable Thomas M. Davis, III, House of Representatives. During the review, we assessed (1) the status of the Navy's efforts to oversee its Year 2000 program and (2) the appropriateness of the Navy's strategy and actions for ensuring that the problem will be successfully addressed. This letter summarizes our concerns and provides recommendations for addressing them.

Results in Brief

The Navy relies on computer systems for some aspect of virtually every operation, including strategic and tactical operations; sophisticated weaponry; intelligence, surveillance, and security efforts; strategic sealift and fleet mobilization and readiness; and routine business functions such as financial, personnel, logistics, and contract management. Failure to address the Year 2000 problem in time could severely degrade or disrupt the Navy's day-to-day and, more importantly, mission-critical operations.

The Navy has taken many positive actions to increase awareness, promote sharing of information, and encourage its components to make Year 2000 remediation efforts a high priority. However, it is behind schedule in remediating systems. For example, the Navy did not finish assessing its

mission-critical systems until December 1997 even though it anticipated that this would be done in June 1997. In addition, it is still in the initial stages of assessing whether Year 2000 fixes are required for computer hardware, communications equipment, security and building systems, and other infrastructure equipment.

Furthermore, the Navy lacks key management and oversight controls to enforce good management practices, direct resources, and establish a complete picture of its progress in remediating systems. For example, the Navy:

- currently lacks a comprehensive departmentwide inventory of systems requiring remediation;
- has not been tracking component progress in developing written agreements with their interface partners;
- has not developed a test strategy for the department; and
- is not developing contingency plans that focus on ensuring the continuity of all of its critical military operations and business processes.

As a result, the Navy lacks complete and reliable information on its systems, and on the status and cost of its remediation efforts. It has also increased the risk that (1) Year 2000 errors will be propagated from one organization's systems to another's, (2) all systems, interfaces, and equipment important to Navy operations will not be thoroughly and carefully tested, and (3) the department will not be prepared if systems are not corrected or replaced by the Year 2000 deadline.

Objectives, Scope, and Methodology

Our objectives were to assess (1) the status of Navy's effort to identify and correct its Year 2000 problem and (2) the appropriateness of the Navy's strategy and actions for remediating Year 2000 problems. In conducting our review, we used our Year 2000 Assessment Guide[1] to assess the Navy's Year 2000 efforts. This guide addresses common issues affecting most federal agencies and presents a structured approach and provides a checklist to aid in planning, managing, and evaluating Year 2000 programs. The guidance, which is consistent with Defense's Year 2000 Management Plan[2] and the Navy's own Year 2000 management approach, describes five phases—supported by program and project management activities—with

[1]Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997); first issued as an exposure draft in February 1997.

[2]Version 2, January 1998.

each phase representing a major Year 2000 program activity or segment. The phases and a description of each follows.

- **Awareness** - Define the Year 2000 problem and gain executive-level support and sponsorship. Establish a Year 2000 program team and develop an overall strategy. Ensure that everyone in the organization is fully aware of the issue.
- **Assessment** - Assess the Year 2000 impact on the enterprise. Identify core business areas and processes, inventory and analyze systems supporting the core business areas, and prioritize their conversion or replacement. Develop contingency plans to handle data exchange issues, lack of data, and bad data. Identify and secure the necessary resources.
- **Renovation** - Convert, replace, or eliminate selected platforms, applications, databases, and utilities. Modify interfaces.
- **Validation** - Test, verify, and validate converted or replaced platforms, applications, databases, and utilities. Test the performance, functionality, and integration of converted or replaced platforms, applications, databases, utilities, and interfaces in an environment that faithfully represents the operational environment.
- **Implementation** - Implement converted or replaced platforms, applications, databases, utilities, and interfaces. Implement data exchange contingency plans, if necessary.

During our review, we concentrated on the Navy's efforts to oversee its Year 2000 program during the awareness and assessment phases—the first two phases of its overall five-phased approach. We focused our review on Year 2000 work being carried out by (1) DOD's Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I), which is responsible for promulgating DOD guidance on Year 2000 matters and providing assistance to Defense components, (2) Navy Headquarters, including the Offices of the Chief Information Officer (CIO), who is responsible for overall coordination and management and for issuing Navy Year 2000 policy and guidance, and (3) the Navy's two largest systems commands, the Naval Air Systems Command (NAVAIR) and the Naval Sea Systems Command (NAVSEA), which are the central activities responsible for developing, acquiring, and supporting aeronautical systems and ships and related weapons and combat systems.

Specifically, we met with the Acting Assistant Secretary of Defense for Command, Control, and Communications and Intelligence, the Principal Director for Information Management, the Director for Information Technology, and other senior staff responsible for Year 2000 issues. We

reviewed Defense's Year 2000 guidance and other documentation on Year 2000 funding, reporting, and date format requirements. We met with the Acting Deputy Chief Information Officer, the Team Leader and Coordinator from the Year 2000 Coordination Office, and the NAVSEA Coordinator and the NAVAIR Deputy CIO. We obtained and analyzed documents issued by these offices that describe organizational structure and responsibilities for carrying out the Navy Year 2000 program. We reviewed the Navy's Year 2000 Action Plan[3] to assess the level of guidance, roles, and responsibilities, and target milestone dates for the Year 2000 effort.

We also reviewed other pertinent Year 2000 program documentation such as Defense and Navy guidance and management directives, working group minutes, status reports, and cost and schedule data. Further, we reviewed available inventory information on the Navy's mission-critical systems contained in the Defense Integration Support Tools (DIST) database, which the Navy uses to help manage its Year 2000 efforts. In doing so, we determined (1) the number of systems reported to be owned and operated by Navy organizations and (2) the reported status of Navy systems in their Year 2000 efforts. We also assessed the reliability and completeness of the Navy's Year 2000 information.

We relied on work previously conducted at the Naval Supply Systems Command (NAVSUP), which is the Navy's primary supply manager. In our report[4] on NAVSUP's Year 2000 efforts, we found that NAVSUP had made considerable progress in meeting its Year 2000 challenges as a result of implementing a centralized management and control approach.

We performed our work primarily at the Navy's Year 2000 Coordination Office and the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence in Arlington, Virginia. We conducted our work from August 1997 through April 1998 in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the Secretary of the Navy. Comments from the department are discussed in the "Agency Comments and Our Evaluation" section and are reprinted in appendix II.

[3]Specifically, we reviewed the Navy's draft plan dated November 1997 and subsequent revisions issued in January and March 1998.

[4]Defense Computers: Technical Support Is Key to Naval Supply Year 2000 Success (GAO/AIMD-98-7R, October 21, 1997).

Background

Most of the Navy's automated information systems and weapons systems are vulnerable to the Year 2000 problem, which is rooted in the way dates are recorded and computed in automated information systems. For the past several decades, systems have typically used two digits to represent the year, such as "97" representing 1997, in order to conserve electronic data storage and reduce operating costs. With this two-digit format, however, the Year 2000 is indistinguishable from 1900, or 2001 from 1901, etc. As a result of this ambiguity, computerized systems and/or application software that use dates to perform calculations, comparisons, or sorting may generate incorrect results when working with years after 1999. In addition, any electronic device that contains a microprocessor or is dependent on a timing sequence may be also vulnerable to Year 2000 problems. This includes computer hardware, telecommunications equipment, building and base security systems, street lights at military installations, elevators, and medical equipment.

Should Navy computer systems fail, Navy operations at all levels could be impacted by the incorrect processing of data as well as corrupted databases or even massive system failures. In turn, this could result in such problems as delays in supply shipments, faulty inventory forecasts, unreliable budget estimates, and erroneous personnel-related information. Moreover, the problem could adversely impact critical maritime operations such as combat, communications, command and control, intelligence, surveillance, reconnaissance, strategic sealift, and fleet mobilization and readiness.

Like the other military services, the Navy has adopted DOD's Year 2000 management strategy, which charges components (that is, program managers and system owners) with responsibility for making sure that all of their systems correctly process dates and gives them the flexibility to implement solutions as they deem appropriate. In December 1995, the Navy designated the Navy Information Systems Management Center with responsibility for (1) coordinating Year 2000 efforts being carried out by its 9 operating forces, including the U.S. Marine Corps, and its 17 shore establishments which include 5 major systems commands, (2) facilitating the sharing of Year 2000 information and best practices departmentwide, and (3) monitoring the Navy's Year 2000 progress. In August 1997, the Navy transferred this responsibility to its newly established Office of the Department of the Navy Chief Information Officer. Appendix I illustrates the Navy's organizational structure and describes the complexity involved in carrying out Year 2000 efforts at the component level.

To comply with DOD's current Year 2000 funding mandate, the Navy is not providing program managers and system owners additional funds to manage and fix the Year 2000 problem. Rather, program managers and system owners have been directed to use previously budgeted funds (that is, primarily operational and maintenance (O&M) funds) or reprogram other programmatic funds to fix Year 2000 problems. As of February 1998, the Navy estimated that it will cost about $421 million to successfully complete its Year 2000 program, but as discussed later, this estimate is not reliable.

The Navy's Year 2000 Efforts to Date

To increase awareness of Year 2000 and to foster coordination among its components, the Navy has taken the following actions.

- In November 1995, it formally began the awareness phase of its Year 2000 program.
- In April 1996, it established a Navy Year 2000 homepage that serves as a clearinghouse for Year 2000 information.
- Since October 1996, it has participated in a number of Year 2000 interface assessment workshops sponsored by Defense. These workshops are designed to acquaint managers with the nature and extent of interface problems pertaining to 21 functional areas, such as finance, intelligence, logistics, communications, and weapons systems.
- From March 1997 through May 1998, it has conducted quarterly reviews to keep abreast of Year 2000 problems. These reviews are attended by representatives from the Secretary of the Navy, the CIO office, and the major Navy and Marine Corps commands and activities. Since May 1998, the Navy CIO office has been holding weekly briefings with the commands.
- In April 1997, it adopted and implemented DOD's compliance checklist to assist system managers in ensuring that their systems are compliant for the Year 2000. The checklist focuses on (1) identification of systems and interfaces, (2) assessment of date usage by the systems, and (3) compliance testing, among other subjects.
- In August 1997, it identified Year 2000 as its highest priority behind life-threatening or mission failure repairs and instructed components to put a higher priority on funding remediation efforts than on other information technology initiatives.
- In December 1997, it tasked the Navy Inspector General to assess Year 2000 readiness at its commands. The IG plans to report on its assessment of 12 commands in April. At the time of our review, the IG had not issued any reports. In February 1998, the Navy requested the Naval Audit Service to review Year 2000 readiness at the commands not visited by the IG.

- In January 1998, it formally issued its Year 2000 Action Plan. The March 1998 revision of this plan sets milestones for the completion of major Year 2000 activities and provides exit criteria for each phase.

In February 1998, the Navy reported to the Office of Management and Budget that it had 812 mission-critical [5] and 1,575 nonmission-critical automated information and embedded systems.[6] According to the Navy, 781 mission-critical systems need to be repaired; about a quarter of these were reported to be in the renovation phase and over half in the validation phase. In addition, the Navy reported that 1,422 nonmission-critical systems need to be repaired; about a third of these were reported to be in renovation and half in validation. Specific reported totals for February 1998 are shown in table 1. As discussed later in this report, we found the Navy's status information to be unreliable.

[5]For Year 2000 purposes, the Navy defines a mission-critical system as "a system that when its capabilities are degraded, the organization will realize a resulting loss of a core capability."

[6]These figures reflect only those systems entered into the DIST database.

Table 1: Reported Status of the Navy's Year 2000 Efforts

	Mission-critical systems		Nonmission-critical systems	
Status	**Number**	**Percent[a]**	**Number**	**Percent[a]**
Total systems	**812**		**1,575**	
Compliant	0	0	0	0
To be replaced before 2000	19	2.3	26	1.7
To be retired before 2000	12	1.5	127	8.1
To be repaired	781	96.2	1,422	90.3
Reported status of systems to be repaired				
Total systems	**781**		**1,422**	
In awareness phase	0	0	0	0
In assessment phase	0	0	33	2.3
In renovation phase	191	24.5	459	32.3
In validation phase	441	56.5	712	50.1
In implementation phase	14	1.8	20	1.4
Corrected[b]	135	17.3	198	13.9

[a]Percentages do not total 100 percent due to rounding.

[b]In late 1997, the Office of the Secretary of Defense established this reporting category to indicate those systems that have completed all five Year 2000 phases. NAVAIR, for example, plans to require the system sponsor to certify its systems as Year 2000 compliant before it can report it as "corrected."

Source: Navy information reported to the Office of Management and Budget. We did not independently verify this information.

In its February 1998 report, the Navy provided the following information on personal computers and communications and facility equipment.

Table 2: Information Reported by the Navy on Other Equipment

	Total inventory	Number compliant	Percent compliant	Number not compliant	Percent not compliant	Number Status unknown
Personal computers/servers	313,781	111,114	35.4	164,241	52.3	38,426
Communication devices (including telecommunications equipment)	13,105	3,428	26.2	2,213	16.9	7,464
Facility devices (includes such items as elevators, security systems, and medical equipment)	3,113	1,925	61.8	471	15.1	717
Total	**329,999**	**116,467**	**35.3%**	**166,925**	**50.6%**	**46,607**

Source: Navy information reported by components. Only compliant systems were reported to the Office of Management and Budget. We did not independently verify this information.

Navy Progress in Early Year 2000 Phases Has Been Slow

The Navy is behind schedule in completing the early phases of its Year 2000 program. For example, although Defense required that all systems be assessed by June 1997, the Navy reported that it did not finish assessing its mission-critical systems until December 1997, and, as of February 1998, reported it was still assessing about 2 percent of its nonmission-critical systems . In addition, it did not issue an approved Year 2000 program management plan until January 1998. Our guide recommends that this be done early in the assessment phase. Further, it is still assessing whether corrective actions are needed for other equipment such as computer hardware, communications equipment, and security systems. In April 1998, the Navy issued a draft assessment guide to evaluate these assets.

Technology experts like the Mitre Corporation and the Gartner Group estimate that organizations should spend less than 30 percent of their effort in the first two phases and reserve 70 percent for the renovation, validation, and implementation phases of the Year 2000 program. Because the Navy has spent about 60 percent of the time available completing the first two phases, it will be difficult to complete the more complex and time-consuming tasks of renovating, testing, and implementing its systems in the time remaining.

Navy officials acknowledge that the assessment phase is taking longer than expected. They attribute this delay to difficulties associated with

developing a complete systems inventory and the lack of skilled field people to perform Year 2000 tasks. Before its Year 2000 effort, the Navy did not have a comprehensive servicewide system inventory nor did many of its components. Therefore, it could not readily determine the magnitude of the Year 2000 problem servicewide or the cost to fix it.

Even though Navy CIO officials acknowledged that the department is behind schedule, the Navy has recently moved up its target completion dates for its mission-critical systems for the remaining three phases.

Table 3: Navy's Accelerated Year 2000 Target Completion Dates for Mission-Critical Systems

Phase	November 1997 draft action plan	March 1998 action plan
Awareness	12/1/96	12/1/96
Assessment	6/30/97	6/30/97
Renovation	8/1/98	6/30/98[a]
Validation	12/30/98	10/30/98
Implementation	5/1/99	12/31/98[a]

[a]OMB's governmentwide target completion date for renovation is September 1998; the target completion date for implementation is March 1999.

Under the accelerated schedule, the Navy plans to complete the renovation phase for mission-critical systems about 1 month sooner than it originally anticipated and the testing phase 2 months earlier than originally anticipated. It also plans to complete the implementation phase 4 months earlier than anticipated and 3 months before OMB's recommended completion date. Based on the latest reported component data, the Navy estimates that only seven mission-critical systems will not meet its new dates.

As the following sections of this report discuss, the Navy is at risk of not meeting its new schedule because it has not yet established key management and oversight controls needed to successfully complete the next phases. Specifically:

- At the time of our review, Navy headquarters as well as some components did not have strong program offices to guide them through the more complex and difficult phases of remediation.
- The Navy still does not have complete and accurate information on systems, the status of remediation efforts, and costs.

- The Navy has not yet identified all system interfaces nor ensured that interface partners are effectively working together to correct interfaces.
- The Navy has not developed an overall strategy for testing its systems.

In addition, Navy operations are at risk because the Navy has not developed contingency plans to ensure that mission functions can be performed if mission-critical systems are not corrected in time.

The Navy Has Not Been Effectively Overseeing and Managing Year 2000 Remediation Efforts

In view of the magnitude of the Year 2000 problem, our Assessment Guide recommends that agencies plan and manage their Year 2000 programs as a single large information system development effort and promulgate and enforce good management practices at the program and project levels. The guide also recommends that agencies appoint a Year 2000 program manager and establish an agency-level Year 2000 program office.

The Navy took a decentralized approach to the Year 2000 effort but it did not initially establish a strong Year 2000 program office to manage it effectively. For example, during our review, the Navy had assigned only five full-time personnel in the office of the CIO to oversee and monitor the Year 2000 progress of more than 2,000 systems and 300,000 personal computers and servers owned by five major systems commands, 17 shore establishments, and 9 operating forces, including the U.S. Marine Corps. By contrast, the Air Force assigned 27 staff to the Year 2000 problem—3 to oversee and implement program and policy changes across the service and 24 to execute the program.[7] According to Navy CIO officials, the office had not managed Year 2000 remediation efforts effectively, and most of the staff's time had been spent reporting the status of component efforts to top managers in the Navy, DOD, and external entities, such as the CIO Council and OMB. For example, at the time of our review, the staff was not validating information being reported by Navy components for completeness and accuracy; assessing component efforts to prioritize systems; or tracking component progress in completing important Year 2000-related activities, such as contingency planning and testing.

Some of the Navy's components also did not support their own efforts with a strong program office. For example, at the time of our review, NAVSEA did not have any dedicated full-time Year 2000 staff at the command level, even though it is responsible for managing more than 350

[7]The three staff assigned to oversee the program work at the Air Force Communications and Information Center (AFCIC), which reports to the Office of the Chief Information Officer. The 24 personnel assigned to execute the program work at the Air Force Year 2000 Program Office at Scott Air Force Base, Illinois, which reports to AFCIC.

systems involving 138 major acquisition programs and 345 ships—all of which are susceptible to Year 2000 problems. NAVAIR, which is responsible for about 870 systems involving over 200 aeronautical-related programs and over 4,600 aircraft, assigned only three full-time staff to work on the command's Year 2000 problem.

The Navy has recently responded to this problem by assigning three additional staff to the CIO Office to help coordinate Year 2000 activities and by establishing a new Year 2000 Project Office for Navy Operations, comprised of 15 staff. As shown in appendix I, the Chief of Naval Operations is responsible for operating forces across all Navy commands and shore activities as well as key functions, such as intelligence, logistics, and training. The office, which will begin operating in June 1998, will be responsible for coordinating the testing efforts of NAVAIR, NAVSEA, the Space and Warfare Systems Command, and fleet commands. However, there are no plans to have either the CIO Office or the new project office validate data reported by the components or assess component progress in prioritizing systems, identifying and correcting interfaces, and developing contingency plans.

The Navy Does Not Yet Have Complete and Accurate Year 2000 Information

According to our Assessment Guide, a key part of the assessment phase is to identify business areas that are critical to the enterprise and, for each area, critical business processes and supporting information systems. In constructing the inventory of information systems, it is important to assess the potential impact on business processes if systems are not fixed on time, to estimate the cost of remediation, and to monitor the progress components are making toward correcting their systems. This provides the necessary foundation for Year 2000 program planning. The Navy, however, does not yet have a complete and accurate inventory or reliable status and cost information. As a result, it does not have a clear picture of its Year 2000 remediation efforts and it cannot reliably prioritize systems for correction, determine what resources it needs, or identify problems that require greater management attention.

Until recently, the Navy's primary source of Year 2000 system inventory information was the Defense-wide database of automated systems, known as the Defense Integration Support Tools (DIST) database.[8] The Navy was using this database to help oversee its Year 2000 efforts and prepare its

[8]At the beginning of its Year 2000 effort, Defense designated DIST as the primary departmentwide Year 2000 tracking tool. Some components, such as the Air Force and the Army, also built their own databases and used them in managing their Year 2000 programs. The Navy decided to rely solely on DIST and did not build a separate database.

quarterly status reports to the Department of Defense, which, in turn, submits the information to the Office of Management and Budget.

In February 1998, due to concerns that extensive and detailed information on all of the Department's mission-critical systems was available on the Internet, ASD/C3I removed DIST from the Internet and classified it as "secret"—meaning that it can only be accessed by personnel with a valid security clearance, job-related "need-to-know," and access to secure computer and communications equipment. As a result, the Navy has no readily accessible central repository of system information to help oversee system fixes or respond to ad hoc requests for Year 2000 information from OMB or Defense. According to the CIO office, the secret classification given DIST has "gravely hindered" its ability to manage the Year 2000 effort.

The Navy plans to resolve this problem by creating a separate unclassified Year 2000 database and making it available by June 1998. As the Navy implements this new database, it will be important for it to correct the data problems we identified in our discussions with command and headquarters officials as well as in our review of selected information from DIST on the Navy's mission-critical systems[9] provided to us by the Defense Information Systems Agency (DISA) database administrator. These problems include the following.

- Of 819 mission-critical systems in the database, 6 systems failed to identify which stage of remediation they were in, 23 did not provide the name of the system or describe its function, and 118 failed to show an expected compliance date.
- In providing the data, DISA did not include cost information because the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence concluded that the data were unreliable. For example, ASD/C3I noted that in some cost estimates, the decimal point was misplaced, overstating some estimates by millions of dollars.
- Our discussions with headquarters and command officials further revealed that the cost estimate was incomplete. For example, NAVSEA officials told us that the Navy was missing cost information for about 95 percent of NAVSEA's 138 major acquisition programs. NAVAIR also indicated that many of its system managers were not reporting costs.

[9]In conducting our review, we were not provided access to the database. However, in response to a request from the House Committee on National Security that we report on the Year 2000 status of Defense's mission-critical systems, DISA provided us with information from the database on the Navy's mission-critical systems, including the name and description of the system, status of remediation, planned versus actual date of compliance, and status of contingency plans. Because this information was generated after the Navy submitted its February 1998 report to OMB, it reflects seven more mission-critical systems than the February status report.

- The reliability of cost information is also questionable because some Navy components are still using a cost formula derived from the Gartner Group and the Mitre Corporation, which recommends multiplying the number of lines of code by $1.10 for automated information systems and by $8 for weapons systems. Defense recommended that components use this formula early in their Year 2000 efforts, but it also recommended that a more detailed cost analysis based on more than 30 cost factors be conducted as components progressed through the assessment phase and learned more about their systems and the resources that would be required to fix them. The difference between the Gartner/Mitre formula and a more reliable analysis of data collected during the assessment phase can be significant. For example, based on the Gartner/Mitre formula, the Navy estimated that it would cost $4.3 million to correct a mission-critical ordnance management system. Based on a detailed cost analysis of data collected during its assessment, the Navy estimated that remediation costs would actually be about $1.75 million—a 59 percent decrease over the original estimate.

  In addition, as the new database is implemented, it will be important for the Navy to routinely validate the information submitted by its components. While it was using DIST, the Navy did not validate the data. Consequently, it had no assurance that the information on its systems, remediation progress, and cost was correct and complete.

Navy Management of Interface Conversions Has Been Ineffective

Navy systems interface with each other as well as with systems belonging to contractors, other federal agencies, and international entities, such as the North Atlantic Treaty Organization and foreign military sales customers. Therefore, it is essential that Navy components ensure that all interfaces are Year 2000 compliant and that noncompliant interfacing partners will not introduce Year 2000-related errors into compliant Navy systems. Our Assessment Guide and DOD's Year 2000 Management Plan recommend that agreements with interface partners be initiated during the assessment phase to determine how and when interface conflicts will be resolved.

The Navy has not managed the identification and correction of its interfaces effectively. First, although the Navy set the goal of completing renovation of its interfaces by June 30, 1998, many components, including the nine NAVAIR and NAVSEA weapon system program offices we contacted during our review, were still in the process of identifying interfaces and assessing whether they need to be corrected. Second, as of February 1998,

the Navy reported to OMB that it had fixed only 5 of the 1,051 interfaces already identified. For the rest, it had not yet determined whether data bridges would be required,[10] negotiated who was responsible for installing and funding the bridges, or developed agreements documenting the method and schedule for correcting the interfaces. Third, the Navy was not using DIST (before it was classified) or any other information tool to track component progress in completing these activities.

The Navy recently asked its Inspector General and the Naval Audit Service to review the completeness of memorandums of agreement as they conduct their Year 2000 assessments at the commands. However, these reviews will be performed on a limited basis—they are not designed to ensure that all mission-critical program managers and system owners have identified their interfaces, taken appropriate measures to fix them, and documented these agreements with their interface partners.

The Navy Is Not Prepared for the Testing Phase

The validation (testing) phase of the Year 2000 effort is expected to be the most expensive and time-consuming. Experts estimate that it will account for 40 to 60 percent of the entire effort.[11] As DOD's Year 2000 Management Plan notes, organizations "must not only test Year 2000 compliance of individual applications, but also the complex interactions between scores of converted or replaced computer platforms, operating systems, utilities, databases, and interfaces."

To mitigate the risks associated with testing, our Assessment Guide calls on agencies to develop validation strategies and test plans. Validation strategies are developed at an organizationwide level to ensure that common test requirements are followed by all locations. Specifically, they describe the test organization's and its components' roles and responsibilities, system/project priorities, a master schedule of high-level test activities for each system/project, and the test resources to be used in carrying out these activities (people, tools, facilities, and contractors). The plan should be sufficiently detailed to allow system/project-specific planning to occur as well as to permit program office tracking of high-level test activity progress. For example, it should have milestones, including completion dates, for application/system acceptance tests, specify project progress metrics, and allocate common test facilities and other resources

[10]Bridging involves receiving information in one format, modifying it, and outputting it in another format, such as receiving the year in a two-digit format, adding century information through the use of an algorithm, and writing the output with a four-digit year.

[11]According to Mitre Corporation and Gartner Group.

among system renovation projects competing for these facilities and resources. Since agencies may need over a year to adequately validate and test converted or replaced systems for Year 2000 compliance, our Assessment Guide recommends that this planning begin in the assessment phase.

The Navy lacks an overall validation strategy that specifies the common criteria and processes components should use in testing their systems. As such, it has no assurance that all systems and interfaces will be thoroughly and consistently tested. For example, in the absence of a validation strategy:

- There is no guidance on who, when, and how tests of the Navy's estimated 10,000 local area networks (LANs) should be conducted. As a result, the Navy Computer and Telecommunications Command, which manages these networks, is relying solely on its vendors to ensure that Navy LANs are Year 2000 compliant. It does not plan to perform end-to-end tests[12] on shore-based LANs or ensure that vendor tests are adequate.[13] One Navy command has found that relying on vendors to ensure that systems are compliant is not enough to mitigate Year 2000 risks. When NAVSUP tested products that vendors claimed were compliant, it found that many were not.
- The Navy does not know how much testing capacity is needed by its components and how much is available even though it has acknowledged that these resources will be in demand. As our Assessment Guide notes, agencies may have to acquire additional facilities in order to provide an adequate testing environment. The longer the Navy waits to begin assessing the need for these facilities, the less time it will have to acquire additional facilities or otherwise ensure that all mission-critical systems can be tested before the Year 2000 deadline.

In addition to lacking a departmentwide validation strategy, we found that two major components—NAVAIR and NAVSEA—had not developed strategies nor were they ensuring that the organizations reporting to them did so. In

[12]The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, interoperate as intended in an environment which faithfully represents the operational (i.e., live production) environment. These interrelated systems include not only those owned and managed by the organization, but also those external systems with which they interface. Generally, end-to-end testing is conducted when one major system in the end-to-end chain is modified or replaced and attention is rightfully focused on the changed or new system. In the case of Year 2000 testing, however, most if not all of the systems in the end-to-end chain will have been modified or replaced. As a result, the scope and complexity of the testing is dramatically increased, as is the difficulty of isolating, identifying, and correcting problems.

[13]The Navy estimates that shipboard LAN end-to-end testing will begin in the spring of 1999.

fact, NAVAIR did not require its program managers and system owners to develop individual Year 2000 test plans.

Business Continuity and Contingency Planning Is Inadequate

To mitigate the risk that Year 2000-related problems will disrupt operations, our recently issued guide on business continuity and contingency planning[14] recommends that agencies perform risk assessments and develop realistic contingency plans during the assessment phase to ensure the continuity of critical operations and business processes. Contingency plans are important because they identify the manual or other fallback procedures to be employed should systems miss their Year 2000 deadline or fail unexpectedly in operation. Contingency plans also define the specific conditions that will cause their activation.

The Navy is not developing contingency plans that focus on ensuring the continuity of all of its critical military operations and business processes. Instead, it is developing plans for only a small portion of its mission-critical systems—specifically those systems that (1) are scheduled for implementation beyond January 1, 1999, (2) do not complete renovation by June 30, 1998, or (3) fail integrated platform testing. The Navy reported that, under these criteria, only 7 of the 812 mission-critical systems currently require a contingency plan. Three of these plans have been completed. The Navy is taking this approach because it believes that it should spend its resources on identifying and fixing Year 2000 problems early and then concentrate its energy on contingency plans for systems for which renovation is going to be delayed.

Preparing contingency plans on this basis is not judicious. First, even if the Navy's mission-critical systems are replaced or renovated in time, there is no guarantee that they will operate correctly. Second, the risk of Year 2000 failures is not limited to the Navy's internal systems. In fact, the Navy depends on information and data provided by other Defense and federal agencies, international organizations, and private contractors whose systems can introduce Year 2000 problems into Navy's systems. It also relies on services provided by the public infrastructure, which are susceptible to Year 2000 problems that could disrupt operations —including power, water, and voice and data telecommunications. Until its contingency planning focuses on this chain of critical dependencies, the

[14]Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, Exposure Draft, March 1998).

Navy will not be able to ensure that it can maintain the basic functionality of its critical operations and core business processes.

Conclusions

Navy operations may be severely disrupted if the Navy does not successfully remediate its mission-critical computer systems before the Year 2000 deadline. While the Navy has taken a number of actions to address this issue, many critical tasks remain to be done in a relatively short period. At this point, the Navy does not know whether it has identified all systems and interfaces; it lacks reliable data on the status and cost of remediation efforts; and it does not know if it has the capacity to handle the demanding task of testing systems, networks, operating platforms, and databases. Despite the fact that these weaknesses have greatly increased the chances that it will not correct its mission-critical systems in time, the Navy is not adequately prepared to respond to unforeseen problems and delays.

Recommendations

We recommend that you direct the Department of the Navy Chief Information Officer to ensure that the Navy Year 2000 Coordination Office is provided with sufficient staff and authority to implement the following recommendations.

- Establish a complete and accurate inventory of its information systems. Ensure that the data problems identified in this report are corrected and routinely validate the information submitted by components to the database.
- Ensure that components have identified and corrected interfaces and developed written memorandums of agreement with interface partners.
- Develop a departmentwide testing strategy that describes program manager and system owner roles and responsibilities, system/project priorities, a master schedule of high-level test activities for each system/project, and the test resources to be used in carrying out these activities (people, tools, facilities, and contractors). Ensure that Navy components develop their own test strategies and require their program managers and system owners to develop individual test plans.
- Ensure that Year 2000 contingency planning focuses on the continuity of all of the Navy's critical military operations and business processes rather than on only a small portion of mission-critical systems.

Agency Comments and Our Evaluation

In written comments on a draft of this report, the Department of the Navy Chief Information Officer (CIO) concurred with all of our recommendations to improve the Navy's Year 2000 program. In response to our recommendations, the Navy agreed to establish a complete and accurate inventory of its information systems, ensure that components have identified and corrected interfaces and developed memorandums of agreement with interface partners, develop a departmentwide test strategy, and ensure that contingency planning focuses on the continuity of critical military operations and business processes. The Navy also stated that it has increased staff in its Year 2000 Coordination Office to 10 full-time employees to help carry out these activities.

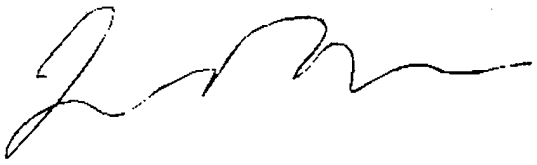
In addition, the Navy noted that its new Year 2000 database, which is expected to be on-line in June 1998, will include additional data elements not contained in DIST, such as actual and programmed costs, planned and actual dates that memorandums of agreements are signed with interface partners, the dates that test plans are prepared, and the status of testing activities. As part of the validation process, the CIO Office plans to conduct weekly reviews of the data for completeness and accuracy. The Navy also stated that, in addition to requiring that contingency plans be prepared on the continuity of business operations and to ensure mission capability at the user level, it is now requiring contingency plans to be prepared for all—rather than a select few—mission-critical systems no later than December 1998.

This report contains recommendations to you. The head of a federal agency is required by 31 U.S.C. 720 to submit a written statement on actions taken on these recommendations to the Senate Committee on Governmental Affairs and the House Committee on Government Reform and Oversight not later than 60 days after the date of this report. A written statement also must be sent to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this report.

We are providing copies of this report to the Chairmen and Ranking Minority Members of the Senate Committee on Governmental Affairs, the Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia, Senate Committee on Governmental Affairs, the Subcommittee on Defense, Senate Committee on Appropriations, the Senate Committee on Armed Services, the Subcommittee on Government Management, Information and Technology, House Committee on

Government Reform and Oversight, the Subcommittee on National Security, House Committee on Appropriations, and the House Committee on National Security. We are also sending copies to the Honorable Thomas M. Davis, III, House of Representatives; the Deputy Secretary of Defense; the Acting Assistant Secretary of Defense for Command, Control, Communications and Intelligence; the Navy Chief Information Officer; and the Director of the Office of Management and Budget. If you have any questions on matters discussed in this report, please call me at (202) 512-6240. Major contributors to this report are listed in appendix III.

Sincerely yours,



Jack L. Brock, Jr.
Director, Governmentwide and Defense Information Systems

Contents

Letter		1
Appendix I Navy Year 2000 Organizational Structure		24
Appendix II Comments From the Department of the Navy		27
Appendix III Major Contributors to This Report		31
Tables	Table 1: Reported Status of the Navy's Year 2000 Efforts	8
	Table 2: Information Reported by the Navy on Other Equipment	9
	Table 3: Navy's Accelerated Year 2000 Target Completion Dates for Mission-Critical Systems	10
Figures	Figure I.1: Department of the Navy Organization Structure	25
	Figure I.2: Example of the Field Structure at One Navy Command	26

Abbreviations

ASD/C3I	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
CIO	Chief Information Officer
IG	Inspector General
DISA	Defense Information Systems Agency
DIST	Defense Integration Support Tools
DOD	Department of Defense
LAN	local area network
NAVAIR	Naval Air Systems Command
NAVSEA	Naval Sea Systems Command
NAVSUP	Naval Supply Systems Command
O&M	operational and maintenance
OMB	Office of Management and Budget

Navy Year 2000 Organizational Structure

As figure I.1 indicates, the size and complexity of the Department of the Navy's organization structure poses a significant management challenge. Year 2000 management and oversight efforts will have to be coordinated among 17 major Navy shore establishments including 5 major systems commands and 9 operating forces, such as the U.S. Marine Corps, the Naval Reserve Forces, the Military Sealift Command, and the Atlantic and Pacific Fleets.

Figure I.2 provides an example of just one command's field structure. To understand the complexity involved in carrying out Year 2000 efforts at the command level, consider the following.

- The Naval Sea Systems Command's fiscal year 1998 budget accounts for about 19 percent (or $15 billion) of the Navy's total budget.
- The Naval Sea Systems Command, which is the largest of five Navy systems commands, employs about 55,000 personnel.
- The command currently manages 138 acquisition category programs assigned to six program executive offices, including Carriers, Littoral Warfare, and Auxiliary Ships; Mine Warfare; Surface Combatants/AEGIS Program; Submarines; Theater Air Defense; and Undersea Warfare.
- The command is responsible for 345 ships, including 92 submarines and 14 aircraft carriers, assigned to 24 home ports in the United States and overseas.
- The command manages about 1,275 foreign military sales cases. Because the command's systems interface with the systems belonging to its foreign military sales customers, it will need to develop interface agreements with its customers.
- The Naval Sea Systems Command alone has about 56 Year 2000 points-of-contacts.

Figure I.1: Department of the Navy Organization Structure

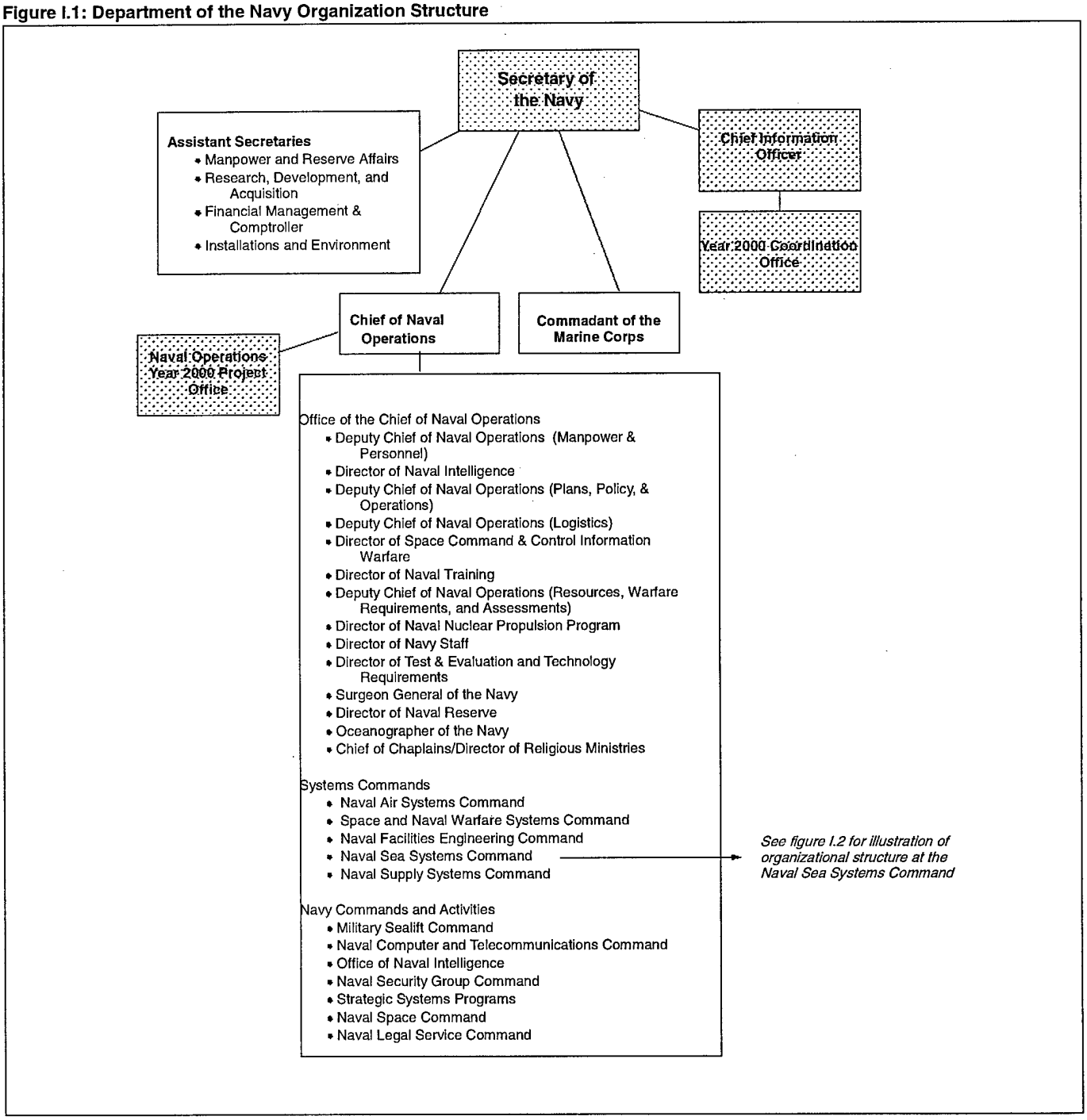
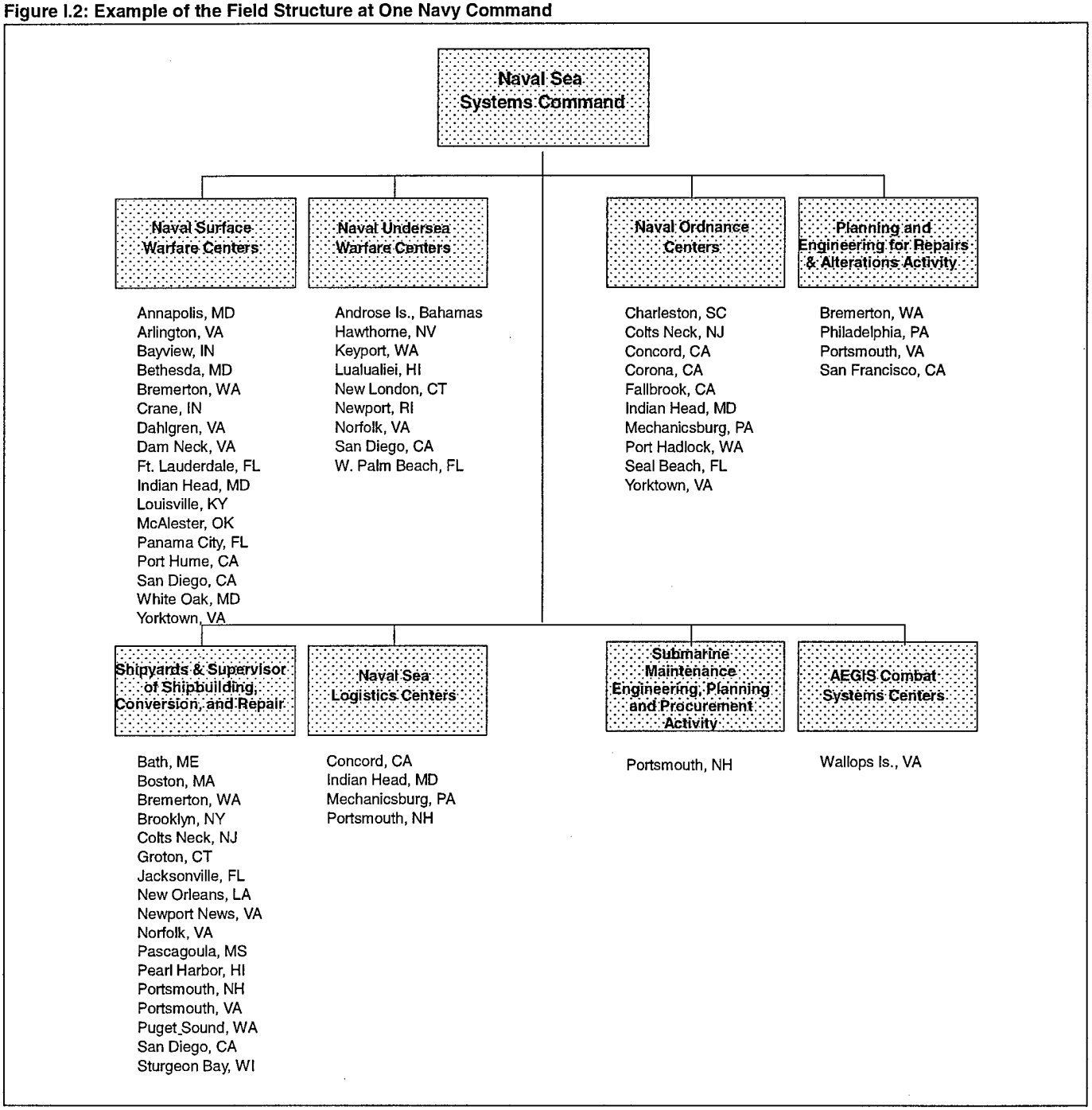


Figure I.2: Example of the Field Structure at One Navy Command



Comments From the Department of the Navy

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

JUN - 8 1998

Mr. Gene L. Dodaro, Assistant Comptroller General
Accounting and Information Management Division
General Accounting Office
Washington, DC 20548

Dear Mr. Dodaro:

One of my highest priorities in the Department of the Navy is to ensure no mission critical system failures occur due to Year 2000 (Y2K) related problems. The impact of the millennium date change on the Department's many information technology systems will be determined largely by the attention we devote to solving the Year 2000 (Y2K) processing problem. To address this issue, my office provided guidance which outlines a centralized management/decentralized execution policy. The Department's Y2K progresses are reported to me weekly by system owners during regularly scheduled briefings.

I also have asked Naval Audit Service and Naval Inspector General to conduct reviews of Y2K status and report their findings to me. These reviews examine Echelon II Commands for proper allocation of resources, for progress against DON and DoD mandated milestones, for contingency plans, for responsibility assignment and identification of system interfaces, for required Memoranda of Agreement, and for use of the Department of the Navy Y2K Database.

Your findings and recommendations have been helpful in identifying necessary changes in our approach to solving this very important challenge. During my short tenure as DON CIO we have accomplished two of the GAO report recommendations and are fully committed to completing the remaining two recommendations. Please let me know if you would like to meet to discuss this issue further. My point of contact is CAPT Clifford Stanley, (703) 602-6882.

Dr. Ann Miller

Attachment: DON Response
Distribution

GAO DRAFT REPORT - DATED MAY 19, 1998
(GAO CODE 511624) OSD CASE 1622

"DEFENSE COMPUTERS: YEAR 2000 COMPUTER PROBLEMS PUT NAVY OPERATIONS AT RISK"

RECOMMENDATIONS

- **RECOMMENDATION 1:** The GAO recommended that the Secretary of the Navy direct the Navy CIO to ensure that the Navy Year 2000 coordination office is provided with sufficient staff and authority to establish a complete and accurate inventory of its information systems. Ensure that the data problems identified in this report are corrected and routinely validate the information submitted by components to the database. (p. 29,GAO Draft Report)

- **DON RESPONSE: Concur -** The DON Y2K team has been operational since May 1996. Since that date the DON CIO Y2K team has grown to10 full time employees. In March 1998, the Navy Y2K Project Office was activated to coordinate Navy Y2K issues. This office is staffed by OPNAV codes with 13 full time employees, and led by a Flag Officer. The Marine Corps Y2K Team coordinates Marine Corps issues and is staffed by 6 full time employees, and led by a Marine Corps Colonel. The DON CIO Y2K Team coordinates both Navy and Marine Corps issues. The DON CIO has also established weekly briefings by the Department of Navy organizations, to identify/rectify problems and/or weaknesses.

  At the time of this GAO audit, the DON was reliant on the Defense Integrated Support Tool (DIST) as its database for Y2K management and reporting. Earlier this year the Office of the Secretary of Defense (OSD) classified the database and it was pulled from use, leaving the DON with no Y2K database. With the classification of the DIST, the DON had to develop an alternative database tool to track and document the current status of Y2K activity. The new DON database will be on-line in June 98. PEOs and PMs will have direct access to the database to provide system, subsystem, interface and cost information including actual, programmed and re-prioritized costs. All levels of the Navy, Marine Corps and the Reserves will have access to the DON Y2K database.

  Weekly reviews of the Y2K database will be conducted by the DON CIO Y2K team (as part of the validation process) for completeness and accuracy.

- **RECOMMENDATION 2:** The GAO recommended that the Secretary of the Navy direct the Navy CIO to ensure that the Navy Year 2000 Coordination Office is provided with sufficient staff and authority to ensure that components have identified and corrected interfaces and developed written memorandums of agreement with interface partners. (p. 29/GAO Draft Report)

- **DON RESPONSE: Concur** - The DON CIO requires all program managers to negotiate memoranda of agreement regarding system to system interfaces. This is an ongoing effort requiring continuous activity. Interface MOA information was never included in the DoD provided DIST database, hence the GAO found the DON lacking in this area. Interface MOA progress will be tracked and reported in the DON Y2K database. Senior level management involvement will ensure that these data elements are populated properly in the new DON database.

  Memoranda of agreement are being developed and tracked for interface partners. The DON database will capture the status of MOAs in three categories: (1) MOAs drafted but not signed, (2) estimated date an MOA will be signed, and (3) the actual date an MOA was signed. Senior management and the DON CIO have noted that interface MOAs with other Government Agencies are necessary and are being pursued.

- **RECOMMENDATION 3:** The GAO recommended that the Secretary of the Navy direct the Navy CIO to ensure that the Navy Year 2000 Coordination Office is provided with sufficient staff and authority to develop a department-wide testing strategy that describes system manager/owner roles and responsibilities, system/project priorities, a master schedule of high level test activities (people, tools, facilities, contractors). Ensure that the Navy components develop their own test strategies and require their system managers/owners to develop individual test plans. (p. 29-30/GAO Draft Report)

- **DON RESPONSE: Concur** - The Navy Y2K Project Office is leading an IPT to develop a Y2K Master Test Plan that will develop all required elements identified by the GAO report. Under the proposed Navy Y2K Test Strategy there are 3-levels of testing: (1) system level testing by program owners (PEOs/PMAs, etc.), (2) functional testing in an operational environment to address functional system integration and, (3) battle group integrated testing afloat. In anticipation of DoD policy on integrated testing, the DON is prepared to provide support to the Joint Staff for development of a DoD wide test plan. The DON Y2K database tracks the existence of test plan information and progress during the validation (testing) phase.

- **RECOMMENDATION 4:** The GAO recommended that the Secretary of the Navy direct the Navy CIO to ensure that the Navy Year 2000 Coordination Office is provided with sufficient staff and authority to ensure that Year 2000 contingency planning focuses on the continuity of all of Navy's critical military operations and business processes rather than on only a small portion of mission-critical systems. (p. 29-30/GAO Draft Report) (p. 29-30/GAO Draft Report)

- DON RESPONSE: Concur - Contingency plans have been identified as an important component of the Y2K management process and are being developed for mission critical systems and some mission support systems. The Navy Y2K Project office is leading a team to coordinate the development of contingency plans to promote continuity of business operations and ensure mission capability at the user level. The Navy Y2K Project office is now requiring contingency plans for all mission critical systems no later than 31 December 1998. The Marine Corps Y2K office already requires contingency plans for all their systems (mission critical and mission support).

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.	John B. Stephenson, Assistant Director Ronald B. Bageant, Assistant Director Cristina T. Chaplain, Communications Analyst Alicia L. Sommers, Senior Information Systems Analyst
Chicago/Dayton Field Office	Steven M. Hunter, Senior Evaluator Robert P. Kissel, Jr., Senior Evaluator Robert G. Preston, Senior Evaluator
Atlanta Field Office	Christopher T. Brannon, Senior Evaluator Teresa F. Tucker, Senior 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. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512 6061, or TDD (202) 512 2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER