

April 1998

DEFENSE COMPUTERS

Year 2000 Computer Problems Threaten DOD Operations





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

**Accounting and Information
Management Division**

B-278156

April 30, 1998

The Honorable Fred Thompson
Chairman
Committee on Governmental Affairs
United States Senate

The Honorable Stephen Horn
Chairman
Subcommittee on Government
Management, Information and Technology
Committee on Government Reform and Oversight
House of Representatives

The Honorable Thomas M. Davis, III
House of Representatives

The Year 2000 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 Department of Defense 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 disruptive to military operations worldwide.

For an organization as large as Defense—with over 1.5 million computers, 28,000 systems, and 10,000 networks—addressing its Year 2000 problem is a formidable task. Several Defense components are larger than most civil agencies and, in addition to the computers themselves, thousands of embedded microprocessors used in a variety of equipment such as telephone switches, traffic control, security, and elevator control systems, and some weapons systems must be checked for Year 2000 vulnerabilities.

In view of the impact this problem can have on warfighting and military support missions, you requested that we review the Department of Defense's program for solving the Year 2000 computer systems problem. In response to your request, we have separately reviewed Year 2000 efforts being carried out by the Army, Navy, and Air Force; the Defense Logistics Agency (DLA); the Defense Finance and Accounting Service (DFAS); the Defense Information Systems Agency (DISA); and three central design

activities.¹ This report assesses (1) the overall status of Defense's effort to identify and correct its date-sensitive systems and (2) the appropriateness of Defense's strategy and actions to correct its Year 2000 problems.

Results in Brief

The Department of Defense relies on computer systems for some aspect of all of its operations, including strategic and tactical operations, sophisticated weaponry, intelligence, surveillance and security efforts, and routine business functions, such as financial management, personnel, logistics, and contract management. Failure to successfully address the Year 2000 problem in time could severely degrade or disrupt any of Defense's mission-critical operations.

Defense has taken many positive actions to increase awareness, promote sharing of information, and encourage components to make Year 2000 remediation efforts a high priority. However, its progress in fixing systems has been slow. For example, the department is still assessing systems even though it originally anticipated this would be done in June 1997. In addition, Defense lacks key management and oversight controls to enforce good management practices, direct resources, and establish a complete picture of its progress in fixing systems. For example:

- There is no program office or full-time executive in charge of the departmentwide effort.
- Information being reported to Defense by components does not provide a reliable indication of program status because it is not being validated for accuracy or completeness.
- Defense has not issued adequate guidance to its components on key issues concerning status reporting, interfaces, and testing.
- Defense has not determined, at the departmentwide level, which systems have the highest impact on its mission.
- Defense is not ensuring that its components are preparing written interface agreements and contingency plans.

As a result, Defense lacks complete and reliable information on systems, interfaces, other equipment needing repair, and the cost of its correction efforts. It is spending limited resources fixing nonmission-critical systems even though most mission-critical systems have not been corrected. 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 and interfaces will

¹The Army's Logistics System Support Center, the Navy's Fleet Material Support Office, and the Air Force's Standard Systems Group.

not be thoroughly and carefully tested, and (3) components will not be prepared should their systems miss the Year 2000 deadline or fail unexpectedly in operation. Each one of these problems seriously endangers Defense chances of successfully meeting the Year 2000 deadline for mission-critical systems. Together, they make failure of at least some mission-critical systems and the operations they support almost certain unless corrective actions are taken.

Objectives, Scope, and Methodology

Our objectives were to determine (1) the overall status of Defense's effort to identify and correct its date sensitive systems and (2) the appropriateness of Defense's strategy and actions to correct these systems. In conducting our review, we used our Year 2000 Assessment Guide to assess Defense's Year 2000 efforts.² This guide addresses common issues affecting most federal agencies and presents a structured approach and a checklist to aid in planning, managing, and evaluating Year 2000 programs. The guidance, which is consistent with Defense's Year 2000 Management Plan³ describes five phases—supported by program and project management activities—with 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 for a Year 2000 program. 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.

²Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997); first issued as an exposure draft in February 1997.

³Version 1.0, April 1997.

- **Implementation** - Implement converted or replaced platforms, applications, databases, utilities, and interfaces. Implement data exchange contingency plans, if necessary.

During our review, we concentrated on Defense's department-level Year 2000 Program, managed by the Assistant Secretary of Defense, Command, Control, Communications and Intelligence (ASD C3I), who is also the Defense Chief Information Officer. To determine how Defense components and their organizations were implementing Defense policy and managing their Year 2000 program efforts, we also reviewed Year 2000 efforts being carried out by Army, Navy, and Air Force headquarters, three Defense agencies, and three central design activities. We also visited a number of other organizations including the Joint Chiefs of Staff, the Global Command Control System (GCCS) Program Office, and the National Security Agency. The scope and methodology of these individual reviews are detailed in the following GAO reports:

- Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998).
- Defense Computers: Technical Support Is Key to Naval Supply Year 2000 Success (GAO/AIMD-98-7R, October 21, 1997).
- Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues (GAO/AIMD-97-149, September 26, 1997).
- Defense Computers: SSG Needs to Sustain Year 2000 Progress (GAO/AIMD-97-120R, August 19, 1997).
- Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems (GAO/AIMD-97-106, August 12, 1997).
- Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem (GAO/AIMD-97-117, August 11, 1997).

Reports on the Army and Navy Year 2000 programs are being developed. We also reviewed efforts by the department to improve the Defense Integration Support Tools database (DIST), which serves as the Defense inventory of automated information systems and is intended to be used as a tool to help Defense components in correcting Year 2000 date problems. The scope and methodology of this work is further detailed in our report, Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort (GAO/AIMD-97-112, August 13, 1997).

In conducting the individual component reviews and assessing oversight efforts from Defense headquarters, we reviewed and analyzed official memoranda and other documents discussing Defense and component Year

2000 policy and procedures; the June 1996 and February 1997 Defense and component responses to Year 2000 questions from the House Government Operations Committee, Subcommittee on Oversight; the January 1997 Action Plan for Year 2000 Information Technology Compliance; Defense's May 1997, August 1997, November 1997, and February 1998 component quarterly reports on Year 2000 program status to ASD C3I, and Defense's subsequent department-level reports to the Office of Management and Budget; Year 2000 status briefings to the Deputy Secretary of Defense by the Military Services, the Joint Chiefs of Staff, DISA, DFAS, and DLA; early drafts and the final April 1997 versions of the Defense Year 2000 Management Plan; and Year 2000 inventory data compiled by ASD C3I, Defense components, and their subcomponents.

We also reviewed and monitored Year 2000 Internet homepages maintained by various contractors, government agencies, ASD C3I, DISA, the Army, the Navy, the Air Force, the Marine Corps, and subcomponents; and minutes of federal, Defense, and Air Force Year 2000 Working Groups. In addition, we held discussions with various Defense Department, component and subcomponent officials concerning Year 2000 problems, corrective actions, and related operational and programmatic impacts of the program. We conducted structured interviews on program policies and practices with Defense Department and component-level Year 2000 program officials. We also reviewed the output of various Defense computer generated databases and management information systems related to Year 2000 activities, but did not verify the integrity of the data in these systems.

Our audit work on this overview report was conducted from August 1997 through February 1998 in accordance with generally accepted government auditing standards.

We requested written comments on a draft of this report from Defense. The Acting Principal Deputy of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence provided written comments, which are discussed in the "Agency Comments and Our Evaluation" section and reprinted in appendix II.

Background

Most of Defense's automated information systems and weapon systems computers are vulnerable to the Year 2000 problem, which is rooted in the way dates are recorded, computed, and transmitted 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, systems or application programs that use dates to perform calculations, comparisons, or sorting may generate incorrect results when working with years after 1999. For example, the Defense Logistics Agency’s Standard Automated Material Management System is used to manage Defense’s vast inventory of supplies. Because it uses dates to automatically target items for deletion, the system erroneously targeted more than 90,000 items for deletion before Defense discovered the problem in 1996.

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. For example, Defense components reported to ASD C3I in February 1998 that more than half of the over 730,000 personal computers they had checked had a Year 2000 problem.

For Defense, the Year 2000 effort is a significant management challenge because it relies heavily on computers to carry out aspects of all operations, and time for completing Year 2000 fixes is short. For example, the department is responsible for more than 1.5 million computers, 28,000 automated information systems, and 10,000 networks. Its information systems are linked by thousands of interfaces that exchange information within Defense and across organizational and international lines. Successful operation after January 1, 2000, requires that Defense’s systems and all of the systems that they interface with be Year 2000 compliant.

Should Defense fail to successfully address the Year 2000 problem in time, its mission-critical operations could be severely degraded or disrupted. For example:

- In an August 1997 operational exercise, the Global Command Control System failed testing when the date was rolled over to the year 2000. GCCS is deployed at 700 sites worldwide and is used to generate a common operating picture of the battlefield for planning, executing, and managing military operations. The U.S. and its allies, many of whom also use GCCS,

would be unable to orchestrate a Desert Storm-type engagement in the year 2000 if the problem is not corrected.

- The Global Positioning System (GPS) is widely used for aircraft and ship navigation (commercial and military) and for precision targeting and “smart” bombs. The ground control stations use dates to synchronize the signals from the satellites and maintain uplinks to the satellites. Failure to correct Year 2000 problems could cause these stations to lose track of satellites and send erroneous information to the millions of users who rely on GPS.
- The Defense Message System (DMS) is being developed to replace the aging Automated Digital Network (AUTODIN). These systems provide critical capabilities such as secure messaging for important operations such as intelligence gathering, diplomatic communications, and military command and control. Should Year 2000 problems render DMS or AUTODIN inoperable or unreliable, it would be difficult to monitor enemy operations or conduct military engagements.
- Aircraft and other military equipment could be grounded because the computer systems used to schedule maintenance and track supplies may not work. Defense could incur shortages of vital items needed to sustain military operations and readiness—such as food, fuel, medical supplies, clothing, and spare and repair parts to support its over 1,400 weapons systems.
- Billions of dollars in payments could be inaccurate because the computer systems used to manage thousands of defense contracts may not correctly process date-related information.
- Active duty soldiers and military retirees may not get paid if the systems used to make calculations and prepare checks are not repaired in time.

Defense’s Year 2000 Efforts to Date

Defense plans to resolve its Year 2000 problem using a five-phased process comparable to that in our Year 2000 Assessment Guide. In keeping with its decentralized approach to information technology management, Defense has charged its components with responsibility for making sure that all of their systems correctly process dates. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD C3I), as the Department’s Chief Information Officer, is responsible for leading Defense efforts to solve the Year 2000 problem. Further, Defense is requiring the components to reprogram existing funds to correct their systems and will provide no additional funds for Year 2000 fixes. As of February 1998, Defense estimated that it would cost \$1.9 billion to address its Year 2000 problem, but as discussed later, we question the reliability of this estimate.

To increase the awareness of the Year 2000 problem and to foster coordination among components, Defense has taken the following actions:

- In a November 27, 1995, memo, the ASD C3I alerted components to the problem and called on them to begin corrective actions if they had not already done so.
- In December 1996, Defense established the Year 2000 Steering Committee, chaired by the Deputy Secretary of Defense, to oversee progress, provide departmentwide guidance, and make decisions related to the Year 2000. Members, which include the department's chief information officers, chief financial officer, general counsel and the acquisition executive also discuss Year 2000 issues and exchange information on their programs. The Steering Committee began meeting in September 1997.
- Defense established a Year 2000 Working Group to support the activities and deliberations of the Steering Committee. The group is chaired by an ASD C3I staff member. Each component has assigned a representative to the group to investigate Year 2000 and cross-functional issues, provide recommendations, identify and share lessons learned, and avoid duplication of effort within Defense.
- In October 1996, the ASD C3I began a series of interface workshops intended to better coordinate Year 2000 efforts in various functional areas. These workshops are intended to ensure information systems and processes that exchange data are assessed and will be Year 2000 compliant. Workshops are conducted for specific functional areas and will continue until Year 2000 problems are resolved.
- In April 1997, Defense issued its Year 2000 Management Plan, which formalized its Year 2000 strategy and delineated the activities involved in each phase of its five-phased approach to remediation. The plan also identified responsibilities of the Year 2000 Steering Committee, the Year 2000 Working Group, the ASD C3I, the Defense Information Systems Agency, and the Assistant Secretary of Defense for Intelligence Systems; established reporting requirements, target completion dates, and exit criteria for each of the program phases; provided guidance on estimating costs; and provided a compliance checklist.
- In May 1997, Defense enlisted its Inspector General to help oversee the department's Year 2000 program, validate the data on Year 2000 status being reported by each component, identify problems areas, and recommend corrective actions.
- In July 1997, a Defense Science Board panel was convened to determine whether the department's strategy, priorities, resources, and funding are sufficient to ensure that all mission-critical systems will be corrected in time.

- Defense has extensively used the Internet to establish Year 2000 home pages, information libraries, and links to other federal and nongovernment Year 2000 organizations, to enhance awareness and understanding of the Year 2000 problem.

In February 1998, Defense reported to OMB that it had 2,915 mission-critical systems and 25,671 nonmission-critical systems. According to Defense, 1,886 mission-critical systems need to be repaired and about half of these are in the renovation phase and a third in the validation phase. In addition, Defense now reports that 15,786 nonmission-critical systems need to be repaired, an increase of over 6,500 systems from the number reported by components in November 1997. Like the mission-critical systems, about half of these nonmission-critical systems are reported to be in the renovation phase.

Defense has taken a long time in the early phases of its Year 2000 program and its progress in fixing systems has been slow. For example, Defense took 16 months to issue its Year 2000 Management Plan, 1 year to establish the Year 2000 Steering Committee, and an additional 9 months for the Committee to hold its first meeting. In addition, Defense is still assessing systems even though it originally anticipated that this would be done in June 1997. In February 1998, Defense reported that only about 130 mission-critical systems had completed repairs since November 1997.

Technology experts like the Mitre Corporation and the Gartner Group, estimate that about 70 percent of an organization's total effort will be required for the renovation, validation, and implementation phases. With less than 20 months remaining and most mission-critical systems in these three phases, Defense is running out of time to make the necessary repairs before the Year 2000 deadline. Specific reported totals for February 1998 are shown in table 1. As discussed later in this report, we question the reliability of this information.

Table 1: Reported Status of Defense Year 2000 Efforts (as of February 1998)

	Mission-critical systems (2,915 systems)		Nonmission-critical systems (25,671 systems)	
	Number	Percent ^a	Number	Percent ^a
Compliant	530	18.3	8,196	31.9
To be replaced before 2000	330	11.3	380	1.5
To be retired before 2000	164	5.6	1,309	5.1
To be repaired	1,891	64.9	15,786	61.5
Reported status of systems to be repaired				
In awareness phase	0	0	4	0.1
In assessment phase	22	1.2	340	2.2
In renovation phase	873	46.2	8,296	52.6
In validation phase	695	36.8	4,241	26.9
In implementation phase	130	6.9	2,644	16.7
Corrected	171	9.0	261	1.7

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

^aPercentages do not total 100 percent due to rounding.

Information on personal computers and communications and facility equipment reported by components is provided in table 2.

Table 2: Information Reported to Defense on Other Equipment

	Total inventory	Compliant	Noncompliant	Unknown
Personal computers	826,762	350,694	381,882	94,186
Communications devices (including telecommunications equipment)	88,166	52,117	17,216	18,833
Facility devices (includes such items as elevators, security systems, medical equipment)	100,421	27,041	14,264	59,116

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

Previous GAO Reviews of Component Year 2000 Efforts

We have separately reported on Year 2000 efforts being carried out by the military services, three Defense agencies, and three central design activities. Our reviews have shown that individual components have also

taken positive actions to increase awareness. For example, the Air Force established an Air Force Year 2000 Working Group comprised of focal points from each major command, field operating agency, and direct reporting unit. The group has focused on such matters as sharing lessons learned, eliminating duplicative efforts, sharing resources, and tracking component progress. Also, the Air Force and other components, such as DFAS and DLA, each developed written Year 2000 plans that adopted the five-phased approach. In addition, these components, as well as some other organizations, such as the central design activities we reviewed, established Year 2000 program offices and designated program managers.

However, there were systemic weaknesses in component Year 2000 programs. For example, many of the components failed to develop contingency plans during the assessment phase to ensure that critical operations can continue in the face of unforeseen problems or delays. They also were not effectively planning to ensure the availability of needed testing facilities and resources. And they had not fully identified interfaces or communicated their Year 2000 plans to their interface partners. Finally, none of the three military services had developed accurate and reliable cost estimates as their systems were assessed. Our findings with regard to these reviews are noted throughout this report and are detailed in appendix I.

Defense Is Not 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 the Year 2000 program as a single large information system development effort and promulgate and enforce good management practices on 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.

Defense has not supported its decentralized approach to the Year 2000 effort with a program manager or an agency-level Year 2000 program office. Instead of establishing a department-level program office, Defense assigned five full-time staff members in the Office of the ASD C3I to oversee the progress of 23 major components and over 28,000 information systems. The group does not have authority to enforce good management practices, direct resources for special needs, or even to question the validity of the data being reported from components.

In addition, this group is not supported by an executive that can focus on the Year 2000 problem full-time. For example, the ASD C3I, who has been

assigned to lead the effort, is also responsible for (1) providing guidance and oversight for all command, control, communications, and intelligence projects, programs, and systems being acquired by Defense and its components, (2) chairing the Major Automated Information System Review Council, (3) serving as the principal Defense official responsible for software policy and practices, and (4) establishing and implementing information management policy, processes, programs, and standards.

Furthermore, Defense has not promulgated and enforced good management practices for Year 2000 corrective efforts. For example, Defense has not provided guidance and authoritative direction needed to ensure that components effectively (1) identify “a system” for purposes of Year 2000 reporting, (2) communicate Year 2000 plans to interface partners, (3) address conflicts between interface partners, and (4) identify common standards and procedures to use in testing. In addition, it has not been validating the information being reported by its components for completeness and accuracy or tracking component progress in completing important Year 2000-related activities, such as contingency planning, acquiring additional test facilities, and prioritizing systems.

Because it lacks strong management and oversight controls over Year 2000 remediation efforts, Defense has failed to successfully address a number of steps that are fundamental to correcting mission-critical systems on time.

- First, Defense does not yet have a complete inventory of systems. Without this, it cannot reliably determine what resources it needs or identify problems requiring greater management attention.
- Second, Defense has not ensured that mission-critical systems are receiving a higher priority than nonmission-critical systems.
- Third, Defense has neither identified all system interfaces nor ensured that its components are effectively working with their interface partners to correct the interfaces.
- Fourth, Defense has not ensured that facilities are available for Year 2000-related testing or that component testing requirements are consistent.
- Fifth, Defense does not know if components have developed contingency plans necessary to ensure that essential mission functions can be performed even if critical mission systems are not corrected in time.
- Sixth, Defense does not have a reliable estimate of Year 2000 problem correction costs.

These weaknesses and their impact on Defense's Year 2000 remediation efforts are discussed in the following sections.

Defense Does Not Have an Accurate and Complete Inventory of Systems

Our Assessment Guide noted that a key part of the assessment phase is to conduct an enterprisewide inventory of information systems for each business area. Such an inventory should include specific information such as the business processes that systems support, the potential impact on those business processes if systems are not fixed on time, and the progress components are making in correcting their systems. This provides the necessary foundation for Year 2000 program planning. Defense, however, does not yet have a complete and accurate inventory of its systems and other equipment needing repair. As a result, it does not have a clear picture of its overall Year 2000 correction efforts and it cannot reliably determine what resources it needs or identify problems that require greater management attention.

Defense is requiring its components to submit quarterly Year 2000 progress reports and to input system information into the departmentwide database of automated information systems, known as the Defense Integration Support Tools (DIST) database. However, many components are still identifying their systems, interfaces, and/or other equipment that may be affected by the Year 2000 problem, such as telecommunications equipment, elevators, and security systems. For example,

- Defense components are still adding systems to the inventory; the total number of nonmission-critical systems increased by over 3,700 systems between November 1997 and February 1998.
- The Air Force, the National Reconnaissance Office, the National Security Agency, and the Under Secretary of Defense for Acquisition and Technology have not yet identified other equipment needing repair such as personal computers and telecommunications equipment.
- Eleven components, including the Defense Information Systems Agency and the Joint Chiefs of Staff, have not yet identified interfaces.

In addition, Defense headquarters does not validate the information it is receiving from its components for accuracy or completeness before reporting its status quarterly to the Office of Management and Budget. Similarly, Navy headquarters does not validate the information being reported by its components and system managers. The Army and the Air Force have enlisted their audit agencies to help validate information being

reported by components. These audits have identified large discrepancies between information maintained by the services and information maintained by individual system owners.

Further, Defense has not provided sufficient guidance to components to ensure they use a common definition of a “system” for reporting purposes. This has further degraded the accuracy of Defense’s inventory reporting. If not precisely defined, one “system” can be interpreted to mean a small application comprised of a few hundred lines of code or the entire collection of systems aboard a major weapon system. At Defense, a variety of interpretations are being used. For example, in August 1997, the Air Force’s F-16 and F-15 weapon system programs reported each system aboard an aircraft (86 and 32 systems, respectively) while the C-17 and B-2 programs treated all onboard systems as a single system. Since each system must be corrected individually, aggregating onboard systems into a single system causes Defense’s inventory to be understated. In addition, while some organizations reported these smaller applications that downloaded and processed information from their major automated information systems, the Defense Logistics Agency did not consider these programs as systems. With some organizations reporting on these systems and others, like DLA, not reporting them, Defense’s inventory is further understating the number of systems that need to be corrected.

Recent Classification of DIST Database Has Further Decreased Its Effectiveness

On February 4, 1998, due to concerns that extensive and detailed information on all of the department’s mission critical systems was available on the Internet, the ASD C3I classified DIST as “secret”—meaning that anyone requiring access to the database must have a validated security clearance and access to secure computer and communications equipment. DIST was removed from the Internet and will remain unavailable until detailed access and security procedures are developed and put in place. As a result, at the close of our review, DIST was not available for system managers to update the Year 2000 status of their systems or determine the status of interfaces or interfacing systems, and Defense and component Year 2000 officials could not use it as a program management tool. In addition, organizations such as the Navy, which rely on the DIST for their only source of inventory information, were directed to create separate databases to meet their quarterly inventory reporting and program management requirements.

In commenting on our draft report, Defense officials told us that ASD C3I was in the process of defining options for a new database to replace DIST.

The new inventory, which Defense intends to be unclassified, would not have as much detailed information on systems as DIST; instead, it would only contain Year 2000-relevant data. ASD C3I officials plan to have the new system in place by mid-summer 1998. Until this new system is in place, Defense will lack a central source for inventory and status information on Defense's Year 2000 program. In addition, the new database will be as ineffective as DIST unless components ensure that the information they submit is accurate and complete and Defense headquarters validates their submissions.

Defense Has Not Effectively Prioritized Systems for Correction

According to our Assessment Guide, an important aspect of the assessment phase is prioritizing the remediation of the systems that have the highest impact on an agency's mission and thus need to be corrected first. This helps an agency ensure that its most vital systems are corrected before systems that do not support the agency's core business.

Defense's Year 2000 plan states that the highest priority should be given to systems that are critical to warfighting and peacekeeping missions and the safety of individuals. The plan makes each component responsible for prioritizing its own systems. This approach is flawed. Since all components' functions are not equally essential to Defense's core missions, Defense cannot define its priorities simply by aggregating components' priorities. For example, as noted in a Defense Science Board report,⁴ Defense has no means of distinguishing between the priority of a video conferencing system listed as mission-critical by one component and a logistics system listed as mission-critical by another component. If it had such a means, the board estimated that the number of "priority mission-critical systems" would be reduced by a factor of 10 or greater.

Once Defense decides the relative priority of its mission-critical systems, it will still need to ensure that its mission-critical rather than nonmission-critical systems receive focused management attention and resources. However, according to its status reports, Defense is correcting nonmission-critical systems nearly as quickly as its mission-critical systems. In February 1998, it reported that 83 percent of its mission-critical systems being repaired were in the renovation or validation phases versus about 80 percent of its nonmission-critical systems.

⁴Interim Report of the Defense Science Board Task Force on Year 2000, January 12, 1998; final report has not yet been issued.

Defense Lacks Assurance That Interfaces Are Being Appropriately Addressed

Defense systems interface with each other as well as with systems belonging to contractors, other federal agencies, and international organizations. For example, supply orders originating from the military services are filled and payments to contractors are made through automated interfaces. Therefore, it is essential that Defense agencies ensure that external noncompliant systems not introduce and/or propagate Year 2000-related errors to compliant Defense systems⁵ and that interfaces function after January 1, 2000.

Defense has held a series of Interface Assessment Workshops for individual functional areas such as finance, logistics, and intelligence in order to raise awareness of the interface problem. While these workshops have helped to acquaint high-level managers with the nature and extent of interface problems, much more effort is needed to assist system managers in making corrections.

First, as noted earlier, the department does not know how many interfaces exist among its systems. Seven of 28 components (25 percent) including the Joint Chiefs of Staff did not report interface information on their February 1998 inventory. In addition, four components, including the National Security Agency and the National Reconnaissance Office reported their interfaces as “to be determined.” Three additional components—including the Navy, Defense Intelligence Agency and Air Force Intelligence—reported interfaces, but had not yet determined whether they were affected by the Year 2000 problem. The longer it takes Defense to identify all interfaces and determine which ones need to be corrected, the greater the risk will be that it will discover too late in its Year 2000 effort that systems will not be able to accommodate the Year 2000 changes from a connecting system.

Second, Defense has not provided sufficiently definitive guidance to establish (1) who is responsible for correcting interfaces and (2) how conflicts—for example, who should fund corrective actions—between interface partners will be resolved. Such guidance is necessary since interface problems will likely cut across command, functional, and component lines and may involve contractors, other government agencies, and international organizations.

⁵An example of this type of problem occurred in July 1997. During a joint operational exercise, system clocks were turned forward to test their ability to handle dates after 1999. One component of Defense’s Global Command and Control System failed to operate properly as a result, and, in turn, began sending error messages to the main computer. These messages caused the main computer to shut down, even though it had not experienced any Year 2000 problems itself.

Finally, in order for interfaces to work, both ends need to know what to send and what to expect. This requires formal documentation of the details on data formats, the timing of format changes, etc. While the April 1997 Management Plan directed components to prepare written agreements with their interface partners, Defense has not provided guidance to its components on what the content of interface agreements should be. Components have been slow in responding to the Management Plans direction. For example, at the time of our review, none of the components we reviewed had completed preparation of all required interface agreements. The Army Year 2000 project office reported that its components were behind in their efforts to do so. Defense components have concurred with our recommendations to date concerning the need to develop interface agreements. However, they are still not being uniformly required across the department. Until these agreements are prepared, Defense components will run the risk that key interfaces will not work.

Defense Is Not Fully 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 45 percent of the entire effort.⁶ As Defense's Year 2000 Management Plan notes, the testing phase will be complex since "components 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, [networks], databases, and interfaces." In some instances, the plan notes, Defense components may not be able to shut down their production systems for testing, and may have to operate parallel systems implemented on a Year 2000 test facility. Also, because over 17,500 systems will require testing prior to the March 1999 testing deadline, it will be important to plan for the use of testing resources carefully.

To mitigate risks associated with testing, our Year 2000 Assessment Guide calls on agencies to develop validation strategies and test plans, and to ensure that resources, such as facilities and tools, are available to perform adequate testing. Validation strategies are developed at an organization-wide level to ensure that common testing requirements are used by all locations. Our Assessment Guide further notes that this planning should begin in the assessment phase since agencies may need over a year to adequately validate and test converted or replaced systems for Year 2000 compliance.

⁶According to the Mitre Corporation and Gartner Group.

Defense lacks an overall validation strategy that specifies uniform criteria and processes which components should use in testing their systems. Defense's Management Plan includes a checklist for certifying Year 2000 compliance, but does not require components to use it. Likewise, a number of major components—including DFAS, the Navy, the Air Force, and the Army—have not developed such strategies nor were they ensuring that the organizations reporting to them did so. As a result, Defense runs the risk that all systems and interfaces will not be thoroughly and carefully tested.

Another important aspect of planning for the test phase is to define requirements for test facilities. As our Year 2000 Assessment Guide notes, agencies may have to acquire additional facilities in order to provide an adequate testing environment. Because of the length and complexity of the testing phase and the potential that facilities may not be available, our guide recommends that this planning begin in the assessment phase. We found that the Navy, the Air Force, the Army had not yet begun this planning. The Defense Information Systems Agency, which operates the Department's central computer centers, has only recently begun assessing what the demand for its facilities will be. The longer Defense waits to begin assessing the demand for and the adequacy of test 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.

Contingency Planning Oversight Is Inadequate

To mitigate the risk that Year 2000-related problems will disrupt operations, Defense's Year 2000 Management Plan and our Year 2000 Assessment Guide recommend that agencies perform risk assessments and develop realistic contingency plans for critical systems and activities. Recent OMB directives⁷ require quarterly reporting of contingency planning activities. 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.

Since many of its systems are critical to mission performance and Defense has fallen behind its own Year 2000 schedule, Defense must develop contingency plans now for essential mission functions. However, although Defense's Year 2000 Management Plan identifies the need for contingency planning to ensure continuity of core processes, Defense is not routinely

⁷OMB's November 1997 quarterly Year 2000 report directs agencies to develop contingency plans and requires that summary contingency plan information be provided to OMB for any mission-critical system that is behind schedule in two consecutive quarterly reports to OMB.

tracking the status of contingency plans or ensuring that its components are developing them. The need for oversight is serious since many of the components we reviewed were not developing contingency plans until we recommended that they do so. For example:

- At the time of our review of their programs, DLA and the Naval Supply Systems Command (NAVSUP) had no contingency plans because they expected that all of their systems would be completed by the Year 2000 deadline and would function correctly. This assumption is not well founded because even if systems are replaced or corrected on time, there is no guarantee that they will operate correctly. In addition, in the event that replacement schedules slip, components may not have enough time to renovate, test, and implement a legacy system or identify other alternatives, such as manual procedures or outsourcing. For example, one system used to help manage DLA's mission-critical \$5-billion a year fuel commodity operations had already slipped 4 to 5 months behind its October 1998 scheduled replacement date. Both DLA and NAVSUP began developing contingency plans after we raised these concerns.
- The Air Force was not tracking the extent to which these plans were being developed by its components for mission-critical systems, and, at the time of our review, five system program offices we surveyed had not prepared such plans. In response to our report, the Air Force began ensuring that contingency plans were developed through Air Force Audit Agency spot checks and management reviews. It also plans to develop contingency plans at crisis response centers as well as incorporate Year 2000 scenarios into existing contingency plans.
- DFAS was preparing contingency planning for noncompliant systems to be replaced before the Year 2000. However, it was not requiring contingency plans for systems being renovated. We noted that DFAS faced a risk that systems being renovated may not be corrected by January 1, 2000, and may not operate correctly even if completed. In response, DFAS began developing contingency strategies for these systems.

In January 1998, the military services briefed the Defense's Year 2000 Steering Committee on the status of contingency planning for mission-critical systems. The Army and Air Force reported that they had completed contingency plans for 49 percent and 30 percent of their mission-critical systems respectively. The Navy is only requiring contingency plans for systems planned to be renovated after June 30, 1998, or implemented after January 1, 1999. Using this criteria and the Navy's current schedule, less than 2 percent of the Navy's 812 mission-critical systems are required to have contingency plans.

Defense Lacks Reliable Cost Information

As Defense's Year 2000 Management Plan and our Assessment Guide state, a primary purpose of the assessment phase is to determine the size and scope of the Year 2000 problem and to prioritize remediation activities. Reliable cost estimates are needed to ensure that adequate resources will be available for Year 2000 activities. Once reliable estimates have been established, they can provide a baseline to measure program progress and to improve future program management. In addition, because Defense is funding Year 2000 efforts from existing budgets, reliable Year 2000 cost estimates are needed to assess the impact on future information technology budgets.

Defense relies on its components to estimate the cost of their Year 2000 efforts, but it has not required that they use a consistent estimating methodology or that they update the estimates when more reliable cost information becomes available during the assessment phase. Defense merely sums up the cost estimates it receives from components to produce the estimate it provides to OMB. As a result, Defense's Year 2000 cost estimate is neither reliable nor complete, and does not provide a useful management tool for assessing the impact of the Year 2000 problem or determining if sufficient resources will be available to complete its fixes.

To make a first rough estimate, Defense suggested that components use 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. This rough estimate was to be refined by conducting a detailed cost analysis based on more than 30 cost factors as the component progressed through the assessment phase and learned more about its systems and the resources that would be required to fix them. These include such factors as:

- the age of systems,
- the skill and expertise of in-house programmers,
- the strategy that the agency is pursuing (strategies that involve keeping the two-digit code, for example, may be much less expensive than those that involve changing the two-digit code to a four-digit code),
- the clarity and completeness of documentation on systems,
- the availability of source code, and
- the programming language used by the systems.

However, Defense did not require that components use these factors in preparing their quarterly cost estimates or that they refine their rough estimates as more reliable information became available during assessment. The difference between an estimate based on a more reliable analysis of data collected during the assessment phase and an estimate based on the Gartner formula and similar methodologies can be significant. For example, in August 1996, the Army's Logistics Systems Support Center used the Gartner formula to project Year 2000 costs for its huge Commodity Command Standard System. Based on this formula, it estimated that it would cost \$8.4 million to correct the system. In April 1997, the Center conducted a detailed cost analysis based on data collected during the assessment phase, and found that Year 2000 costs would actually be about \$12.4 million—a 50 percent increase over the original estimate.

While Defense's Management Plan suggested that components revise their cost estimates as more reliable information becomes available, it has not ensured that components are doing so. While some components may have refined their estimates with each report to the Office of the Secretary of Defense (OSD), the Army, the Air Force, and the Navy continue to provide only rough order-of-magnitude estimates using the Gartner formula or other formulas provided by contractors, or have omitted significant cost items from their estimates. For example:

- The Army's November 1997 estimate of \$429 million did not include costs for 36 systems.
- The Navy's November 1997 estimate of \$293 million did not include cost information from about 95 percent of the program managers in the Naval Sea Systems Command. Naval Air Systems Command also indicated that many program managers were not reporting costs. The Navy estimate also did not include an estimated \$15 million associated with fixing telephone switches.
- The Air Force's November 1997 estimate did not include the cost of fixing telephone switches, which was estimated to be between \$70 million and \$90 million.

Until Defense has a complete and reliable cost estimate, it will not be able to effectively allocate resources, track progress, make trade-off decisions, or resolve funding disputes.

Conclusions

Defense operations hinge on the department's ability to successfully fix its mission-critical computer systems before the Year 2000 deadline. Yet Defense has left it up to its components to solve the problem themselves without establishing a project office, led by a full-time top-level executive, to (1) enforce good management practices, (2) prioritize systems across the department based on criticality to core missions, (3) provide guidance on areas that components should be addressing consistently and ensure that they are doing so, (4) direct resources for special needs, and (5) ensure that data being reported to the Office of Management and Budget and the Congress is accurate. As a result, Defense lacks complete and reliable information on systems, interfaces, and costs. It is allowing nonmission-critical systems to be corrected even though only a small percentage of mission-critical systems have been completed. It lacks assurance that facilities will be available for testing. And, it has not ensured that essential mission functions can be performed if critical mission systems are not corrected in time. Until Defense supports remediation efforts with adequate centralized program management and oversight, its mission-critical operations may well be severely degraded or disrupted as a result of the Year 2000 problem.

Recommendations

We recommend that the Secretary of Defense:

- Establish a strong department-level program office led by an executive whose full-time job is to effectively manage and oversee the Department's Year 2000 efforts. The office should as a minimum have sufficient authority to enforce good management practices, direct resources to specific problem areas, and ensure the validity of data being reported by components on such things as progress, contingency planning, and testing.
- Expedite efforts to establish a comprehensive, accurate departmentwide inventory of systems, interfaces, and other equipment needing repair. Require components to validate the accuracy of data being reported to OSD. Provide guidance that clearly defines a "system" for Year 2000 reporting purposes.
- Clearly define criteria and an objective process for prioritizing systems for repair based on their mission-criticality and ensure that the "most" mission-critical systems will be repaired first.
- Ensure that system interfaces are adequately addressed by (1) taking inventory and assigning clear responsibility for each, (2) tracking progress in Year 2000 problem resolution, (3) requiring interface agreement documentation, and (4) providing guidance on the content of interface agreements and who should fund corrective actions.

-
- Develop an overall, departmentwide testing strategy and a plan for ensuring that adequate resources, such as test facilities and tools, are available to perform necessary testing. Ensure that the testing strategy specifies the common criteria and processes that components should use in testing their systems.
 - Require components to develop contingency plans to ensure that essential operations and functions can be performed even if mission-critical systems are not corrected in time or fail due to Year 2000 problems. Track component progress in completing these plans.
 - Prepare complete and accurate Year 2000 cost estimates so that the department can assess the full impact of the Year 2000 problem, ensure adequate resources are available, and effectively make trade-off decisions to ensure that funds are properly allocated.

Agency Comments and Our Evaluation

In reviewing a draft of this report, the Acting Principal Deputy of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence concurred with all of our recommendations to improve Defense's Year 2000 program. Specifically, Defense agreed with the need to establish a strong central Year 2000 program office and has appointed a full-time executive to lead the department's efforts to solve the Year 2000 challenge. Defense stated that this office will have sufficient authority to enforce good management practices. In addition, Defense stated that the DoD Year 2000 Management Plan is being revised to (1) define criteria and processes for prioritizing systems, (2) formalize guidance on identification and documentation of interfaces, (3) establish common testing conditions and dates for attaining Year 2000 compliance, and (4) provide for development of contingency plans in accordance with GAO's recently issued guidance.⁸ The revised Management Plan is scheduled to be issued in April 1998.

However, in concurring with several of our recommendations, Defense did not indicate how it would implement them. Instead, it reiterated current practices which to date have not resulted in reliable and complete inventory, progress, and cost data. For example, Defense concurred with our recommendation to establish an accurate departmentwide inventory of its systems and a clear definition of the term "system." But, it then said that components will continue to validate the accuracy of data submitted for its new database using audit agencies and other independent validation techniques recommended by OMB and claimed that it had already clearly

⁸Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19 Exposure Draft, March 1998).

defined the term “system” in a March 1997 memorandum from ASD C3I and in DOD’s Dictionary of Military and Associated Terms. Components have not submitted accurate data to Defense to date, and these actions do not indicate that Defense will validate these data to ensure their accuracy in the future as we recommended. Further, the documents cited do not define the term “system” effectively and, as we reported, components have interpreted the term inconsistently.

Likewise, Defense concurred with our recommendation that the Secretary of Defense prepare complete and accurate Year 2000 cost estimates, but then cited current cost estimating guidance and procedures, and noted that it had “requested the Components to improve their estimated costs by using actual figures as they became available.” It added that the Secretary of Defense, through the Year 2000 Steering Committee, will use these estimates to assess the impact of Year 2000 problems, make trade-off decisions, and ensure adequate resources are available. Again, these actions describe current practices which have resulted in incomplete and inaccurate cost estimates. Despite requests from Defense that they refine their cost analyses and prepare complete cost estimates, components continued to provide unreliable and incomplete cost data. Until Defense takes additional action to implement our recommendation to require and ensure that components use a more reliable methodology and report complete costs, it will not have the reliable information it needs to allocate resources, track progress, make trade-off decisions, and resolve funding disputes.

We are providing copies of this letter to the Ranking Minority Members of the Senate Committee on Governmental Affairs and the Subcommittee on Government Management, Information and Technology, House Committee on Government Reform and Oversight; the Chairmen and Ranking Minority members of 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 National Security, House Committee on Appropriations; and the House Committee on National Security. We are also sending copies to the Deputy Secretary of Defense; the Acting Secretary of Defense for Command, Control, Communications and Intelligence; the Director of the Office of Management and Budget; the Assistant to the President for Year 2000; and other interested parties. Copies will be made available to others on request.

If you have any questions on matters discussed in this letter, please call me at (202) 512-6240. Other major contributors to this report are listed in appendix III.

A handwritten signature in black ink, appearing to read "J. Brock, Jr.", with a long horizontal flourish extending to the right.

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

Contents

Letter	1
Appendix I GAO Reviews of Defense Component Year 2000 Efforts	28
Appendix II Comments From the Department of Defense	35
Appendix III Major Contributors to This Report	41
Tables	
Table 1: Reported Status of Defense Year 2000 Efforts	10
Table 2: Information Reported to Defense on Other Equipment	10

Abbreviations

AMC	Army Materiel Command
ASD C3I	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
AUTODIN	Automated Digital Network
CCSS	Commodity Command Standard System
CMM	Capability Maturity Model
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DIST	Defense Integration Support Tools
DLA	Defense Logistics Agency
DMS	Defense Message System
DOD	Department of Defense
FMSO	Fleet Material Support Office
GCCS	Global Command Control System
GPS	Global Positioning System
LSSC	Logistics Systems Support Center
NAVSUP	Naval Supply Systems Command
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
SSG	Standard Systems Group

GAO Reviews of Defense Component Year 2000 Efforts

Department of the Air Force

Report: Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998).

Year 2000

Actions: The Air Force is relying on its components to identify and correct Year 2000 problems affecting their systems, but it has taken a centralized management approach to important assessment activities, such as compiling a system inventory and prioritizing systems for conversion or replacement. It has also charged 24 full-time personnel with responsibility for improving management control and oversight for the Year 2000 program and assigned three full-time headquarters staff members to oversee the Air Force's Year 2000 program. In addition, the Air Force has engaged the Air Force Audit Agency to review specific aspects of its Year 2000 program.

GAO

Findings: We found that the Air Force had not yet refined its cost estimate using actual assessment data (e.g., the age of systems being corrected, the skill and expertise of in-house programmers, and the clarity and completeness of documentation available on the systems), so that it can make informed resource trade-off decisions. We also found that the Air Force had not ensured that components (1) properly identified and corrected interfaces, (2) communicated their interface changes to their data exchange partners, (3) developed contingency plans, and (4) anticipated the need for testing resources.

Recommendations: The Air Force agreed with our recommendations to ensure that (1) future cost estimates factor in the actual resources it believes are needed to renovate and implement systems, (2) an approach is developed to continually track how components are going about identifying and correcting interfaces as well as communicating their interface plans to data exchange partners, (3) components are developing test plans and identifying the need for testing resources, and (4) components have prepared contingency plans for mission-critical systems.

Naval Supply Systems Command

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

Year 2000

Actions: At the time of our review, Naval Supply Systems Command (NAVSUP) was using the services of its primary central design activity--the Navy Fleet Material Support Office (FMSO)--to aid in developing and implementing Year 2000 systems solutions and to supplement the Year 2000 management and oversight of the command. This office had been assessed by an independent external entity as a Capability Maturity Model (CMM) level 3 development organization, indicating that it can realistically plan and manage software development maintenance projects across the organization in a disciplined manner.

GAO

Findings: We found that the command had not (1) allocated sufficient resources to the FMSO Year 2000 Project Office to ensure that all systems interfaces were identified and adequately monitored for progress and (2) directed that risk assessments be performed or that contingency plans be prepared. After we raised these concerns, NAVSUP and FMSO officials assigned full-time staff to identify and correct interfaces. It also began requiring systems managers to perform risk assessments and develop contingency plans.

Recommendations: Because NAVSUP and FMSO acted on our concerns during our review, we did not make specific recommendations to strengthen their Year 2000 program.

Logistics Systems Support Center, Army Materiel Command

Report: Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues (GAO/AIMD-97-149, September 26, 1997).

Year 2000

Actions: The Logistics System Support Center (LSSC) is one of several central design activities for the Army Materiel Command (AMC). Its major responsibility is to design, develop, integrate, and maintain the Commodity Command Standard System (CCSS)--a standard automated wholesale logistics system. CCSS consists of 561 separate subsystems that contain 10.2 million lines of code in about 5,000 programs. These subsystems work collectively to process an annual procurement budget for supplies and equipment of over \$23 billion. At the time of our review, LSSC had inventoried its systems, established a Year 2000 task force, acquired automated software assessment tools, and designated a project manager and Year 2000 management staff. It was also regularly reporting on CCSS' Year 2000 status to AMC headquarters.

GAO

Findings: LSSC had not assigned enough qualified staff to fix CCSS and had not scheduled enough time for testing. In addition, the memoranda of agreement LSSC was developing to communicate its Year 2000 plans to interface partners were inadequate in that they did not specify (1) points of contacts, (2) the date the agreement becomes effective, and (3) the type of correction being used at each end of the interface. Further, LSSC had not yet developed a contingency plan for CCSS.

Recommendations: In response to our report, DOD agreed to develop a contingency plan for CCSS. It began reducing and prioritizing LSSC's current workload to ensure that Year 2000 issues received more attention and it began increasing staff with the necessary skills to help ensure the timely completion of the Year 2000 project. It also extended the completion date for testing from November 1998 to October 1999. And it ensured that interfaces agreements contained information we reported as missing.

Standard Systems Group, Air Force Electronic Systems Center

Report: Defense Computers: SSG Needs to Sustain Year 2000 Progress
(GAO/AIMD-97-120R, August 19, 1997).

Year 2000

Actions: Standard System Group (SSG) is a component of the Air Force Electronic Systems Center and is the central design activity for 137 standard computer programs. Among these, 90 are at risk of failure due to the Year 2000 problem. SSG has achieved a CMM level 3, meaning that it can realistically plan and manage software development and maintenance projects across the organization in a disciplined manner. SSG convened a working group to examine the Year 2000 problem. It developed a Year 2000 strategy, established a Year 2000 project office, and developed a Year 2000 project plan. It also developed a technical guide for system managers to address the problem.

GAO

Findings: Prior to our review, the SSG Year 2000 project office had not been identifying and monitoring the status of individual system interfaces. Also, it was not effectively communicating its Year 2000 plans to its interface partners. After we raised concerns, SSG assigned additional qualified staff to monitor the progress of Year 2000 systems interface resolutions and to communicate Year 2000 plans to interface partners.

Recommendations: Because SSG began acting to more effectively manage the Year 2000 conversion of its interfaces, we made no specific recommendations.

Defense Information Systems Agency

Report: Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort (GAO/AIMD-97-112, August 13, 1997).

**Year 2000
Actions:**

This review focused on the Defense Information System Agency's (DISA) efforts to improve the Defense Integration Support Tools (DIST) database--which serves as the DOD-wide inventory of automated information systems. Defense is using DIST as a primary departmentwide Year 2000 tracking tool. In addition, some components, such as the Navy, are using the DIST as their systems inventory. Others, such as the Army and Air Force, maintain their own inventory databases but they update their portion of the DIST as well. DISA and the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence recognized that DIST was not sufficiently reliable or accurate to manage the Year 2000 effort. As a result, they initiated efforts to (1) improve the integrity of DIST inventory information, (2) facilitate access to information within the database, and (3) ensure that services and components input information needed to complete the inventory.

**GAO
Findings:**

DIST was not being improved quickly enough to be used effectively for Year 2000 remediation efforts. Without a complete inventory, Defense could not adequately assess departmentwide progress toward correcting the Year 2000 problem and address crosscutting issues--such as whether system interfaces were being properly handled and whether there was a need for additional testing facilities. In addition, components that were using DIST as their inventory could not adequately monitor the progress of their own efforts.

Recommendations: In concurring with our recommendations, Defense instituted a data quality program for DIST to, among other things, purge duplicative and obsolete data and assist users in completing system entries as necessary. Defense also agreed to perform statistical sampling of DIST data to validate accuracy, and to rely on the DOD inspector general to validate DIST data accuracy during its Year 2000 audits.

Defense Logistics Agency

Report: Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems (GAO/AIMD-97-106, August 12, 1997).

Year 2000

Actions: The Defense Logistics Agency (DLA) completed its awareness and assessment phases in February 1997; inventoried its systems; conducted pilot projects to determine Year 2000 effects on some of its major systems; and developed and issued policies, guidelines, standards and recommendations on Year 2000 remediation for the agency.

GAO

Findings: DLA had not

- formally documented interface agreements;
- included smaller, unique computer applications (i.e., those applications not developed by DLA headquarters which downloaded and processed data from DLA's major automated information systems) in its inventory;
- prioritized major systems to ensure that mission-critical systems were corrected first; and
- developed contingency plans.

Recommendations: Defense concurred with our recommendations to (1) require written interface agreements between DLA and its interface partners, (2) prepare contingency plans for critical systems, and (3) take inventory of its smaller, unique computer applications. However, it did not agree with our recommendation that the DLA CIO, the Chief of the Customers Support Team and the Systems Design Center Command prioritize systems in conjunction with system customers. Rather, it contended that delegating this responsibility to its business areas was sufficient. As noted in our report, this approach is flawed since all business areas are not equally essential to DLA's core mission.

Defense Finance and Accounting Service

Report: Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem (GAO/AIMD-97-117, August 11, 1997).

Year 2000

Actions: At the time of our review, Defense Finance and Accounting Service (DFAS) had appointed a project manager to provide Year 2000 guidance and track progress; established a Year 2000 systems inventory; implemented a quarterly tracking process to report the status of individual systems; estimated the cost of renovating systems; begun assessing its systems to determine the extent of the problems; and started to renovate and test some applications.

GAO

Findings: DFAS' Year 2000 plan did not address actions needed to complete the testing and implementation phases. It also did not establish milestones for meeting critical tasks under each phase. In addition, DFAS had not

- developed contingency plans for systems it was renovating,
- identified all system interfaces or completed written agreements with interface partners, and
- defined what Year 2000 test facilities it expected to use and ensured their availability.

Recommendations: Defense concurred with all of our recommendations to improve the DFAS Year 2000 program. Among other things, these recommendations called on DFAS to update its Year 2000 plan to ensure that it identified the actions and established the schedules for completing each phase of the Year 2000 program; strengthen contingency planning; require timely identification of all system interfaces and the preparation of written interface agreements; and identify test facilities and resources needed to test systems.

Comments From the Department of Defense

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000



March 27, 1998

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

Dear Mr. Dodaro:

This is the Department of Defense (DoD) response to the General Accounting Office (GAO) draft report, "DEFENSE COMPUTERS: Year 2000 Computer Problems Threaten DoD Operations and National Security," dated March 10, 1998 (GAO Code 511636/OSD Case 1562).

The recommendations contained in the report are valid and in many cases had been recognized by the Components. Some remedial actions had been started before the General Accounting Office made their initial recommendations. There are, however, some areas of the report that require editing. These are noted in the Department's "Additional Comments".

The Department appreciates the opportunity to respond to the GAO recommendations. Your support in our efforts to both aggressively and comprehensively meet the Year 2000 challenge is essential. Should additional information be required, the point of contact for this action is Ms. Edna Campbell, (703) 614 6784.

Sincerely,

Anthony M. Valletta
Acting Principal Deputy

Enclosures



See comment 1.

Appendix II
Comments From the Department of Defense

GAO DRAFT REPORT - DATED MARCH 10, 1998
(GAO CODE 511636/OSD CASE 1562)

"DEFENSE COMPUTERS: YEAR 2000 COMPUTER PROBLEMS THREATEN DOD
OPERATIONS AND NATIONAL SECURITY"

DEPARTMENT OF DEFENSE

RECOMMENDATIONS AND DOD RESPONSES

RECOMMENDATION 1: The GAO recommended that the Secretary of Defense establish a strong department-level program office led by an executive whose full-time job is to effectively manage and oversee the Department's Year 2000 efforts. The office should as a minimum have sufficient authority to enforce good management practices, direct resources to specific problem areas, and assure the validity of data being reported by components on such things as progress, contingency planning, and testing. (p. 36-37/GAO Draft Report)

DOD RESPONSE: Concur. The Secretary of Defense agrees a strong program office is needed and has appointed a full-time executive and resources to lead the Department in its efforts to solve the Year 2000 challenge. The office will have sufficient authority to enforce good management practices, assist in directing resources, and validate, with the assistance of the DoD Inspector General and other DoD audit entities, the data being reported.

RECOMMENDATION 2: The GAO recommended that the Secretary of Defense expedite efforts to establish a comprehensive, accurate department-wide inventory of systems, interfaces, and other equipment needing repair. Require components to validate the accuracy of data being reported to OSD. Provide guidance that clearly defines a "system" for Year 2000 reporting purposes. (p. 37/GAO Draft Report)

DOD RESPONSE: Concur. The Defense Integration Support Tools (DIST) was to be the Department's comprehensive inventory of systems and interfaces. The aggregation of information on the Department of Defense's information technology inventory, interfaces and other pertinent data has been evaluated by the National Security Agency as an unacceptable threat to the security of the United States. Consequently, the Acting

1

03/31/98

Now on p. 22.

Now on p. 22.

Appendix II
Comments From the Department of Defense

ASD(C3I) limited access to the DIST in January 1998, and classified it at the Secret level on February 4, 1998.

On March 20, 1998, DoD initiated action to immediately establish a similar but unclassified Y2K interactive database that will allow the Department to collect validated information to evaluate progress and provide the quarterly report to Office of Management and Budget.

Components will continue to validate the accuracy of reported data. Audit agency requirements and other independent validation techniques recommended by the Office of Management and Budget will assist in ensuring the compilation of valid Y2K information. Validation techniques include: (1) testing by operation and maintenance contractors, independently validated through pilot testing done by the owner of the system; (2) contractor developed and tested systems that are acceptance tested by the owner; and (3) validation of methodologies and test results by the owners' audit agencies.

DoD has provided guidance on definitions in a number of venues. The definition for "Y2K system" is contained in the March 12, 1997, memorandum from the Assistant Secretary of Defense, Command, Control, Communications and Intelligence. The official DoD definition of "system" is in Joint Pub 1-02, DoD Dictionary of Military and Associated Terms. Either of these definitions provides clear guidance.

RECOMMENDATION 3: The GAO recommended that the Secretary of Defense clearly define criteria and an objective process for prioritizing systems for repair based on their mission criticality and ensure that the "most" mission critical systems will be repaired first. (p. 37/GAO Draft Report)

DOD RESPONSE: Concur. The DoD Y2K Management Plan Version 1 contains broad guidance on prioritizing systems and Version 2, scheduled for release in April 1998, will provide expanded direction. In addition, the Secretary of Defense will define criteria and a process for prioritizing systems for repair based on the needs and mission of the Department of Defense. This process will be implemented no later than June 30, 1998.

RECOMMENDATION 4: The GAO recommended the Secretary of Defense ensure that system interfaces are adequately addressed by (1)

2

03/31/98

Now on p. 22.

Appendix II
Comments From the Department of Defense

Now on p. 22.

taking inventory and assigning clear responsibility for each, (2) tracking progress in Year 2000 problem resolution, (3) requiring interface agreement documentation, and (4) providing guidance on the content of interface agreements and who should fund corrective actions. (p. 37/GAO Draft Report)

DOD RESPONSE: Concur. Great strides have been made in identifying interfaces both internal and external to the Department. The reporting process developed in response to Office of Management and Budget is in place to provide a quarterly snapshot of the DoD status in repairing Y2K impacted systems. All DoD Components are implementing memoranda of agreement with each of their interface partners that define at the minimum the interface format, target date for implementation, Point of Contact, address, telephone, and signature of both partners. Through the DoD Year 2000 Work Group, OSD has provided sample memoranda to the Components. This informal guidance will be formalized in Version 2 of the Y2K Management Plan.

Now on p. 23.

RECOMMENDATION 5: The GAO recommended that the Secretary of Defense develop an overall, department-wide testing strategy and a plan for ensuring that adequate resources, such as test facilities and tools, are available to perform necessary testing. In addition, the GAO recommended the Secretary of Defense ensure that the testing strategy specifies the common criteria and processes components should use in testing their systems. (p. 38/GAO Draft Report)

DOD RESPONSE: Concur. The Defense Information Systems Agency (DISA) and the Joint Interoperability Test Command (JITC) has originated a series of testing conditions and dates to attain compliant status for the Department's AISS. In addition, a minimum date set that should be tested will be included in Version 2 of the DoD Y2K Management Plan.

RECOMMENDATION 6: The GAO recommended that the Secretary of Defense require components to develop contingency plans to ensure that essential operations and functions can be performed even if mission critical systems are not corrected in time or fail due to Year 2000 problems.

DOD RESPONSE: Concur. Contingency plans will be developed in accordance with the new GAO Year 2000 Computing Crisis:

3
03/31/98

Appendix II
Comments From the Department of Defense

Business Continuity and Contingency Planning Exposure Draft, dated March 1998.

DoD Components are required to prepare a component-wide master contingency plan which would allow continued operation should there be failures resulting from the Y2K problem. This contingency plan should be based on several disaster scenarios, including failure of the national infrastructure that provides power to facilities.

In addition, contingency plans for individual mission critical AISs must be developed based on each Component's master plan. Contingency planning should be completed no later than September 30, 1998, and will be reviewed quarterly.

RECOMMENDATION 7: The GAO recommended that the Secretary of Defense prepare complete and accurate Year 2000 cost estimates so that the Department can assess the full impact of the Year 2000 problem, ensure adequate resources are available, and effectively make tradeoff decisions to ensure that funds are properly allocated. (p. 38/GAO Draft Report)

DOD RESPONSE: Concur. The Assistant Secretary of Defense, Command, Control, Communications and Intelligence (ASD(C3I)) in Version 1 of the DoD Year 2000 Management Plan adopted a cost algorithm of \$1.10 per executable line of code (ELOC) for AISs and of \$8.00 per ELOC for embedded chips and weapons systems. These algorithms were developed by private industry and adopted by the Department. Further guidance from the ASD(C3I) requested the Components to improve their estimated costs by using actual figures as they became available.

The Secretary of Defense will use these estimates to assess the impact of the Y2K problem and, through the DoD Year 2000 Steering Committee, will make tradeoff decisions as necessary to fund repairs of mission critical systems. In this manner, the Department of Defense will assure adequate resources are available to address Y2K issues.

Cost estimates derived using this methodology are submitted to the Office of Management and Budget as part of the Department's quarterly report.

4
03/31/98

Now on p. 23.

Appendix II
Comments From the Department of Defense

The following is GAO's comment on the Department of Defense's March 27, 1998, letter.

GAO Comment

1. Defense's additional comments have been incorporated as appropriate but have not been included in the report.

Major Contributors to This Report

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

John B. Stephenson, Project Director
Keith A. Rhodes, Technical Director
Ronald B. Bageant, Assistant Director
Carl M. Urie, Assistant Director
Madhav Panwar, Technical Assistant Director
Brian C. Spencer, Technical Assistant Director
Alicia L. Sommers, Senior Information Systems Analyst
Brenda A. James, Senior Information Systems Analyst
Robert L. Crocker, Senior Information Systems Analyst
Cristina T. Chaplain, Communications Analyst

Atlanta Field Office

Carl Higginbotham, Senior Information Systems Analyst
Christopher T. Brannon, Staff Evaluator
Teresa Tucker, Senior Information Systems Analyst

Chicago/Dayton Field Office

Robert P. Kissel, Jr., Evaluator-in-Charge
Steven M. Hunter, Senior Evaluator
Robert G. Preston, Senior Evaluator
Thomas Hewlett, Staff Evaluator

Denver Field Office

John A. Spence, Information Systems Analyst

Kansas City Field Office

George L. Jones, Senior Information Systems Analyst
Denice M. Millett, Senior Evaluator
Michael W. Buell, Staff Evaluator
Karen S. Sifford, 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. 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>

**United States
General Accounting Office
Washington, D.C. 20548-0001**

**Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100**

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

