
May 1998

DEFENSE COMPUTERS

Army Needs to Greatly Strengthen Its Year 2000 Program





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

**Accounting and Information
Management Division**

B-278864

May 29, 1998

The Honorable Robert M. Walker
The Acting Secretary of the Army

Dear Mr. Secretary:

This report presents the results of our review to date of the Army's program for solving its Year 2000 computer systems problem. The problem results from the inability of computer programs at the year 2000 to interpret the correct century from a recorded or calculated date having only two digits to indicate the year. Unless corrected, this problem could cause systems to 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 Army and other Department of Defense (DOD) operations.

We performed this work as part of our review of DOD's Year 2000 computer systems efforts for the Chairman of the Senate Governmental Affairs Committee; 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. Our objectives were to assess (1) the status of the Army's efforts to identify and correct its systems and (2) the appropriateness of the Army's strategy and actions to remediate its Year 2000 problems. This letter summarizes our concerns and provides recommendations for addressing them.

Results in Brief

The Army relies on computer systems for virtually every aspect of its operations including strategic and tactical operations, sophisticated weaponry, and routine business functions such as financial, personnel, logistics, and contract management. Failure to successfully address the Year 2000 problem in time could severely degrade or disable Army mission-critical operations.

The Army has taken many positive actions to increase awareness, promote sharing of information, and encourage components to make Year 2000 remediation efforts a high priority. It has also enlisted the services of the Army Audit Agency (AAA), the Army Inspector General, and various contractors to help evaluate component needs and identify areas that could impact the successful completion of the Army's Year 2000 program.

However, it 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, at the time of our review, the Army

- did not have complete and accurate information on systems, interfaces, and the costs and progress of remediation efforts,
- had not completed interface agreements and contingency plans, and
- had not determined how much testing capacity was needed and available.

Each of these problems seriously endangers the Army's chances of successfully meeting the Year 2000 deadline for mission-critical systems. For example, without good status and cost information, the Army cannot effectively (1) ensure that all its mission-critical systems are being corrected, (2) identify areas where additional resources are needed, (3) ensure that Year 2000 errors are not propagated from one organization to another, or (4) assess whether systems have been certified as compliant. Without prompt attention to interface agreements and contingency plans, there is an increased risk that key interfaces will not work and that core business processes will be adversely impacted. Without knowing at the department level how much testing capacity is needed and available, the Army will not be able to help acquire additional resources in the event that insufficient capacity is available to meet its needs. Together, these problems greatly increase the risk of failure of some mission-critical systems and operations unless corrective actions are taken.

Army officials recognize that improvements in the Year 2000 program are needed and have recently taken actions directed at ensuring that the year 2000 does not pose a threat to the Army's ability to execute its mission. For example, in commenting on a draft of this report, the Army Chief Information Officer (CIO) stated that, due to our audit efforts and those of military audit agencies, he has required, through a policy memorandum, that Army components (1) inventory all system interfaces and coordinate interface agreements with interface partners, (2) complete contingency plans, (3) certify the compliance of systems, and (4) provide more complete and accurate systems data. The CIO also indicated that he is scheduling individual Year 2000 progress reviews with senior-level component managers during the April-May 1998 time frame to review their efforts to fix Year 2000 problems. While we are encouraged by these actions, until all corrective actions have been completed, the Army cannot ensure that it will successfully meet the Year 2000 challenge.

Scope and Methodology

In conducting our review, we assessed the Army's Year 2000 efforts against our Year 2000 Assessment Guide.¹ 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 the DOD Year 2000 Management Plan² and the Army's own Year 2000 guidance,³ describes five phases—supported by program and project management activities—with each phase representing a major Year 2000 program activity or segment. The guide draws heavily on the work of the CIO Council Subcommittee on Year 2000, and incorporates guidance and practices identified by leading organizations in the information technology industry. The phases and a description of each phase 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 operational environment.
- **Implementation**—Implement converted or replaced platforms, applications, databases, utilities, and interfaces. Implement data exchange contingency plans, if necessary.

To determine the status of the Army's Year 2000 program and the appropriateness of its strategy and actions for ensuring successful completion, we evaluated DOD's Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD/C3I) efforts to provide Year 2000 support to the Army. We also

¹Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997). The guide was initially issued in February 1997 as an exposure draft.

²Version 1.0, April 1997.

³U.S. Army Project Change of Century Action Plan (Revision I, October 4, 1996).

evaluated the efforts of the Army's Office of the Director of Information Systems, Command, Control, Communications, and Computers (DISC4) to manage and oversee Army components' correction of the Year 2000 problem. The DISC4 Director also serves as the Army CIO. Specifically, we obtained and reviewed from these offices pertinent Year 2000 guidance, project and funding documentation, and date format requirements. In addition, we reviewed the U.S. Army Project Change of Century Action Plan to assess the level of guidance, roles, and responsibilities and target milestone dates for the Year 2000 effort. Further, we met with Army officials and analyzed their efforts to address the Year 2000 problem at the Army Materiel Command (AMC)—one of the Army's 17 major commands.

We also obtained a copy of the Army's October 1997 Year 2000 inventory database to evaluate its accuracy, reliability, and usefulness. The Army relies on this database to monitor Year 2000 progress and as the source of Army information input to the Defense Integration Support Tools. We also reviewed segments of the Year 2000 database that AMC uses to manage its Year 2000 program. However, because the results of limited data testing showed that these Army databases were incomplete and inaccurate, we could not and did not rely on the data to validate Year 2000 costs or the numbers of systems reported as being in each Year 2000 phase. We also obtained a copy of the U.S. Army Year 2000 Database User's Manual and discussed the specifics of database use and effectiveness with Army officials.

In addition, we met with officials from the Logistics Systems Support Center (LSSC), an Army central design activity with responsibility for maintaining the software for the Commodity Command Standard System (CCSS)—a large standard automated information system—to determine whether LSSC officials were receiving Year 2000 guidance and other related requirements issued by the OASD/C3I and the Army's DISC4. We also discussed with LSSC officials their progress and challenges they face in solving the Year 2000 problem. Further, we compared the information they maintained on their efforts with the information DISC4 and AMC are maintaining for oversight purposes. Lastly, we obtained and analyzed Army and AMC data to gain an understanding of the size, complexity, and diversity of the Army's Year 2000 organizational structure. To help ensure that we were not duplicating other audit agency work, we met with officials of AAA and the Army Inspector General to determine the objectives and scope of their reviews of the Army's Year 2000 problem. We also discussed preliminary results of work performed on the Army's Year 2000 inventory database with AAA officials.

We conducted our work primarily at the Army's DISC4 office in Fairfax, Virginia; AMC Headquarters in Alexandria, Virginia; and LSSC in St. Louis, Missouri. Our work was performed from November 1996 through February 1998 in accordance with generally accepted government auditing standards. This work builds upon information included in a series of DOD component-level Year 2000 reports that have already been issued, including a related report on the Army LSSC.⁴ We requested and received written comments on a draft of this report from the Chief Information Officer of the Department of the Army. These comments are discussed in the "Agency Comments and Our Evaluation" section and are reprinted in appendix II.

Background

Many of the Army's automated information systems and embedded 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. However, with this two-digit format, the year 2000 is indistinguishable from 1900, as is 2001 indistinguishable from 1901. As a result of this ambiguity, system or application programs that use dates to perform calculations, comparisons, or sorting may generate incorrect results when working with years after 1999.

Should the Army's computer systems fail on the morning of the Year 2000, Army 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 weapons systems failures, delays in supply shipments, faulty inventory forecasts, unreliable budget estimates, and erroneous personnel-related information. The problem could also lead to a degradation of the Army's ability to maintain a readiness posture by seriously slowing or curtailing its ability to sustain the warfighters' vital supplies and information.

⁴Defense 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: Improvements to DOD Systems Inventory Needed for Year 2000 Effort ([GAO/AIMD-97-112](#), August 13, 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).

Like the other military services, the Army has adopted the DOD Year 2000 management strategy, which calls for centralized oversight with decentralized execution of Year 2000 corrective actions. The strategy also adopts DOD's five-phased management approach for addressing the Year 2000 problem. The Army has assigned responsibility to DISC4 for overseeing the Year 2000 effort and has charged it with facilitating the sharing of information and best practices and with monitoring Army Year 2000 progress. DISC4 is the Army's primary information resources manager and its director also serves as the Army's CIO. As of October 1997, the Army Year 2000 Project Office had eight staff to oversee the Army's Year 2000 program. Appendix I shows the Army's Year 2000 organizational structure and depicts the complexity and diversity of the Year 2000 program. It also provides an example of the magnitude of the Year 2000 effort at a major command level.

Current Status of the Army's Year 2000 Program

The Army began its Year 2000 program in December 1995 by establishing a Year 2000 Project Office. Although an official charter was never formulated, the Army Year 2000 Project Office was tasked with broad responsibility for providing centralized oversight and management of the Army's Year 2000 effort. In March 1996, the Army approved an initial U.S. Army Project Change of Century Action Plan. This plan, which was revised in October 1996, formalized the Project Office's responsibilities, which include

- establishing Army-wide strategies and guidance for addressing the Year 2000 problem;
- overseeing Army-wide Year 2000 planning and monitoring progress;
- representing the Army in Year 2000 discussions with DOD and other government agencies;
- developing a strategy for Army Year 2000 cross-functional resource decisions;
- directing the establishment of Year 2000 emergency response teams trained and capable of rapidly responding to and assisting with critical operational systems that fail due to Year 2000 problems;
- chairing an Army Year 2000 Working Group to (1) investigate Year 2000 and cross-functional issues, (2) avoid duplication of effort, (3) identify and share lessons learned, and (4) provide recommendations for Army-wide improvement; and
- establishing and maintaining Army Year 2000 home pages (public and restricted) that contain the Army Year 2000 systems database and serve as a clearinghouse for Year 2000 information.

At the time of our review, the Army Year 2000 Project Office had already met many Year 2000 challenges. For example, the Project Office had (1) developed an extensive Year 2000 plan that specified tasks, goals, and milestones for each phase of Year 2000 corrective actions, (2) established roles and responsibilities for performing the specified tasks, (3) provided guidance to components for estimating Year 2000 costs, and (4) published Year 2000 certification requirements. The Year 2000 plan was updated in October 1996 and revised in January 1998.⁵ The Project Office had conducted six Army-wide data calls to accumulate important Year 2000 information from its components. Early in the awareness phase, it had also established a baseline system inventory that was used to develop and populate the Army's current Year 2000 system inventory database. The Project Office's establishment of an Army Year 2000 home page enables Army components to access systems inventory information. Throughout the effort, the Project Office has maintained its Year 2000 awareness campaign and has emphasized to Army organizations the need to report Year 2000 information.

In early 1997, the Army took several actions to minimize the adverse impact of the Year 2000 problem. The Army's CIO requested that AAA help evaluate component needs and identify areas that could cause Year 2000 failures. At the time of our review, AAA had completed Phase I of its eight-phase audit coverage and was finishing detailed site work on Phase II. During Phase I, AAA focused on component oversight and management of Year 2000 issues and the accuracy, completeness, and utility of the Army's Year 2000 inventory database. In the next phases, AAA will assess component progress in remediating, testing, and implementing systems. This work will include determining the reasonableness of the Army's plans for Year 2000 testing and contingency planning. Also, the Army Inspector General is charged with determining the impact of the Year 2000 on personal computers and network hardware, local computer programs and applications, and installation infrastructure⁶ at the tactical unit and installation level. Further, the Army reports that it has supplemented its Year 2000 program with contractor staff that are to concentrate on evaluating the Year 2000 compliance of Army infrastructure items, such as telephone and network switching equipment.

⁵As of January 8, 1998, the U.S. Army Year 2000 (Y2K) Action Plan (Revision II), was still in draft form; however, components have been instructed to adhere to its requirements.

⁶Installation infrastructure includes computerized devices such as traffic signals, elevators, security systems, and heating and ventilation systems located on Army installations.

In February 1998, the Army reported that it had 376 mission-critical automated information and embedded weapons systems and 19,731 nonmission-critical systems. According to the Army, 120 mission-critical systems needed to be repaired; all of these had completed the assessment phase and most were in the renovation phase. In addition, 12,120 nonmission-critical systems needed to be corrected; a small number of these were in the assessment phase and over half were in renovation. As of February 1998, the Army estimated that it would cost \$366 million to address its Year 2000 problem. Specific totals reported by the Army are shown in table 1. As discussed later in this report, we question the reliability of this information.

Table 1: Reported Status of Army Year 2000 Efforts (as of February 14, 1998)

Reported status of systems	Mission-critical systems (376)		Nonmission-critical systems (19,731)	
	Number	Percent	Number	Percent
Compliant	160	42.6	6,699	33.9
To be replaced before 2000	78	20.7	83	0.5
To be retired before 2000	18	4.8	829	4.2
To be repaired	120	31.9	12,120	61.4
Reported status of systems to be repaired				
In awareness phase	0	0	0	0
In assessment phase	0	0	67	0.5
In renovation phase	92	76.7	6,300	51.9
In validation phase	14	11.7	3,245	26.8
In implementation phase	10	8.3	2,505	20.7
Corrected	4	3.3	3	<0.1

Source: Army information reported to OASD/C3I. We did not independently verify this information.

Army Management of the Year 2000 Project Is Ineffective

Although the Army has taken a number of positive steps toward meeting the challenges of the Year 2000 problem, it is not effectively managing its Year 2000 project. First, it lacks complete and accurate information on systems, interfaces, Year 2000 costs, and the progress of remediation efforts. Until these data are complete and reliable, the Army will not have the necessary foundation for managing the Year 2000 program. Second, the Army is late in preparing interface agreements. As a result, there is increased risk that key interfaces will not be corrected prior to the year 2000. Third, the Army is behind in developing contingency plans. Without these plans, it will not be able to minimize the impact of Year 2000

problems on operations. Fourth, the Army has not assessed how much testing capacity is needed and available. As a result, it is missing opportunities to help ensure that all mission-critical systems will be tested before the Year 2000 deadline.

The Army Lacks Complete and Accurate Information Needed to Effectively Manage Year 2000 Remediation Efforts

Our Year 2000 Assessment Guide, Office of Management and Budget (OMB) guidance, and DOD's Year 2000 Management Plan recognize that a key part of the assessment phase is conducting an enterprisewide inventory of information systems for each business area. This inventory should include specific information, such as the business processes the systems support, the potential impact on those business processes if systems are not remediated on time, the schedule for remediation efforts, the identification and descriptions of internal and external system interfaces, and the costs of remediation. This provides the necessary foundation for Year 2000 program planning.

The Army lacks the accurate and complete data required to effectively manage the Year 2000 effort. Specifically, we found that the departmentwide systems inventory maintained by the Army Year 2000 Project Office is unreliable due to (1) poor design of the Army's inventory database and (2) lack of complete information on interfaces, costs, and certifications of Year 2000 compliance. In addition, we reviewed the inventory maintained by the Army Materiel Command (AMC) and found that the component lacked data on systems, costs, and funding.

Inventory Database Is Poorly Designed

The Army's inventory database consists of 139 data fields for each system, including hardware make and model and system software; mission criticality; system owners; the number of executable lines of source code; cost estimates for repair or replacement; schedule for repair; business impact; status certification; and core business areas supported by the systems. Of the 139 data fields, 24 are binary; that is, they have possible values of only "yes" or "no." If any of these fields are left blank, they default to a "no" answer, which may be incorrect. For example, if a system has been designated as mission-critical, but the binary field for this information is left blank, the inventory will show that the system is not mission-critical. This logic flaw could lead to inaccurate information. Although we did not determine the extent to which inaccuracies may have occurred, Army Year 2000 Project Office officials and AAA considered this to be a problem and believed that this flaw put the reliability of inventory data into question.

Interface Information Is Incomplete

Although Army components have identified 1,009 system interfaces that will be impacted by the Year 2000, the Army lacks most of the detailed interface information it needs to monitor and oversee component efforts to ensure that systems data can be exchanged effectively at the year 2000. For example, detailed interface information describing the (1) transfer media (e.g., satellite link, telephone dialup, or diskette), (2) frequency of data exchange (e.g., real time or scheduled periodically), (3) security classification (e.g., unclassified, confidential, or secret), and (4) whether the interface is planned or currently exists had not been provided to the Project Office for the vast majority of interfaces identified. Specifically, of the 1,009 interfaces identified,

- 809 were missing data on transfer media,
- 915 were missing frequency of data exchange information,
- 917 were missing security classification information, and
- 911 did not identify whether the interface is planned or currently exists.

Cost Information Is Both Incomplete and Unreliable

At the time of our review, the Army reported that it expected to spend about \$429 million to correct its Year 2000 problem. However, this estimate was incomplete because (1) it did not contain cost data for all noncompliant mission-critical systems and (2) it was not based on a detailed cost analysis. Of the 143 mission-critical systems requiring repair at the time of the October 1997 quarterly report, 45 percent had costs entered by system managers and 52 percent had no costs entered into the Army's inventory database. The costs of the remaining 3 percent were unknown and were not reported in the \$429 million. However, for the 52 percent of the systems where costs had not been entered into the Army's inventory database by system managers, Year 2000 Project Office staff computed the costs using the Gartner Group formula. This formula recommends multiplying the number of lines of code to be converted by \$1.10 for automated information systems and by \$8.00 for weapon systems. DOD recommended that components use this formula early in their Year 2000 effort to make a rough estimate of costs. However, 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 more was learned about its systems and the resources that would be required to fix them. These include such factors as the

- age of systems;
- 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.

The difference between an estimate based on a reliable analysis of data collected during the assessment phase and an estimate based on the Gartner formula can be significant. For example, using the Gartner formula, in August 1996 the Army LSSC initially estimated that it would cost \$8.4 million to correct CCSS. When it conducted a detailed cost analysis in April 1997 based on data collected during the assessment phase, it estimated that it would cost about \$12.4 million—almost 50 percent more than the August 1996 estimate.

Recently, the Army Year 2000 Program Manager agreed that components need to provide better cost estimates on Year 2000 remediation efforts and indicated that some improvement had been made. For example, the Program Manager told us that, in January 1998, the Project Office had to calculate cost estimates for only about 30 percent of the components' systems compared to calculating cost estimates for over 50 percent of the components' systems in October 1997. However, while progress is being reported, in many cases, the Gartner formula is still being used to calculate cost estimates.

Information Attesting to
Successful Completion of Year
2000 Efforts Is Lacking

To provide assurance that systems are thoroughly tested, properly documented, and determined to be compliant, the Army is requiring that components complete a compliance checklist of all mission-critical and major systems at the conclusion of the validation phase. Once checklists are completed, the components are to submit them to the Army Year 2000 Project Office. While the Army recommends that checklists also be completed for systems that are not mission-critical or major, components are not required to submit completed checklists for them to the Project Office.

At the time of our review, the Army Year 2000 Project Office had not received compliance checklists for any of the 832 mission-critical and major systems contained in its Year 2000 database, including 344 systems that components had identified as Year 2000 compliant. In addition, although checklists are to be submitted to the Project Office after a system has entered the implementation phase, completed certification checklists

had not been received for 30 systems reported to be in the implementation phase. Army officials recently informed us that as of March 31, 1998, 15 certification checklists had been received by the Year 2000 Project Office.

Information Is Also Missing at the Component Level

We reviewed the systems database maintained by AMC—the command responsible for developing, buying, and maintaining equipment and supplies for U.S. soldiers and allies worldwide. AMC data have a significant impact on the Army's Year 2000 effort because AMC and its components own approximately 93 percent of the systems the Army reported as not being Year 2000 compliant. We found that the AMC database lacked important data. For example, 328 of the 505 AMC systems needing Year 2000 remediation did not have repair cost estimates. One of these was the Maneuver Control System—a mission-critical system used for planning, coordinating, and managing battlefield tactical operations. As a result of the missing cost data, AMC's \$196.7 million cost estimate for its Year 2000 remediation program was understated. We also found that another major system, the Munitions Transportation Management System, which helps ensure that correct supplies of munitions are efficiently and effectively transported from port to port worldwide, was missing from the database altogether.

All of these data problems seriously impair the Army's ability to effectively manage Year 2000 remediation efforts. For example, the Army cannot monitor the progress of remediation efforts, identify areas requiring greater management attention, or adequately analyze and prioritize systems conversion or replacement. Without complete interface information, the Army cannot ensure that Year 2000 errors are not propagated from one organization's system to another's. Without good cost information, the Army cannot make informed choices about information technology priorities and determine whether other system development efforts should be deferred or cancelled so that resources can be freed to solve the Year 2000 problem. Without documentation on certification, the Army cannot assess whether systems have been verified as compliant.

Because the Army Year 2000 Project Office did not have effective mechanisms in place to track whether system managers were providing complete and accurate information and to follow up where they were not, the Army is taking action to improve its oversight of Year 2000 efforts. Specifically, AAA and the Army and DOD Inspectors General are engaged in efforts to help determine the extent of data problems and validate the accuracy and completeness of components' information. In addition, in

October 1997, the Army hired a contractor to improve the inventory database by creating an Internet web-based version of the database on the Army Year 2000 home page that is intended to be easier for the user to update and download. Further, the Army CIO and the Army Chief of Staff have been communicating to system managers the need to provide complete and accurate data. While all actions have not yet been completed, these efforts should help encourage better reporting on the part of components and provide the more comprehensive and continued oversight that is needed to establish a complete and accurate picture of remediation efforts. However, the Army Year 2000 Project Office will still need to continuously validate the data submitted by components to ensure the accuracy, completeness, and currency of information in the Army Year 2000 database.

Army Does Not Have Interface Agreements in Place for All Critical Systems and Activities

For system interfaces to work, both sending and receiving interface partners need to know what to send and what to expect from the other. For example, one system manager may choose to make a system Year 2000 compliant by expanding to a four-digit year date, while another may choose to keep the two-digit format and use procedural code or sliding windows as a strategy.⁷ According to current DOD guidance, either fix is acceptable, but both parties need to be aware of the differences and any potential conflicts so that they can install the proper data bridge.⁸

Our Year 2000 Assessment Guide and DOD's Year 2000 Management Plan recommend that written memorandums of agreement (MOA) with interface partners be initiated during the assessment phase to allow enough time for conflicts to be resolved. However, although the Army reports that all of its mission-critical and major systems have completed the assessment phase, as of January 1998, Army components reported that, of the 627 instances where they had identified the need for interface agreements, only 366 MOAs had been completed. In addition, while AAA is in the process of reviewing the existence and quality of components' MOAs, these efforts have not yet been completed at all locations. Until all MOAs have been prepared and the

⁷*Procedural code* is software that derives the correct century based on the two-digit year (e.g., any year smaller than year 50 is a 2000 date and any year 50 or larger is a 1900 date). Like procedural code, *sliding windows* derive the correct century based on the two-digit year, but the numeric constant used to determine the century changes each year. Using the procedural code example above, in the current year, 50 or larger would be a 1900 date, while next year, 51 or larger would be a 1900 date.

⁸*Bridging* involves receiving information in one format, modifying it, and outputting it in another format, such as receiving the year in two-digit format, adding century information through the use of an algorithm, and writing the output in four-digit format.

quality assessed by AAA, the Army is at risk that key interfaces will not work.

The Army Has Not Completed All Contingency Plans

To mitigate the risk that Year 2000-related problems will disrupt critical business operations, DOD's Year 2000 Management Plan, our Year 2000 Assessment Guide, and recent OMB directives recommend that agencies perform risk assessments and develop realistic contingency plans for core business functions during the assessment phase. 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 operations. Contingency plans also define the specific conditions that will cause their activation.⁹

While the Army has issued guidance requiring that contingency plans be prepared for all critical systems and activities, it has not yet completed the development of these plans. As of January 1998, of its reported 344 noncompliant mission-critical and major systems, the Army reported that contingency plans had been completed for 96 systems, no plans had been completed for 82 systems, and the status of the remaining 166 systems was unknown. Army Year 2000 Project Office officials recently informed us that AAA is reviewing contingency plans as part of its Year 2000 reviews of individual systems. While we view AAA efforts as a positive step, if the Army does not ensure that contingency plans for all core business areas are promptly completed and reviewed, it may not have enough time to identify alternatives if replacement or repair schedules slip or systems do not operate correctly. Thus, it will increase the risk of being unprepared to carry out operational missions after the Year 2000 deadline.

The Army Is Not Assisting Components in Identifying, Obtaining, and Scheduling the Use of Test Facilities

The validation (testing) phase of the Year 2000 effort is expected to be the most expensive and time-consuming. For example, the Mitre Corporation, the Gartner Group, and other industry experts estimate that testing will account for 40 percent to 60 percent of the cost of the entire effort. Our Year 2000 Assessment Guide cautions that agencies may need over a year to adequately test converted or replaced mission-critical systems for Year 2000 compliance. Further, as both DOD's Year 2000 Management Plan and our Year 2000 Assessment Guide state, 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

⁹To assist agencies in managing the risk of potential Year 2000-induced disruptions to their operations, we recently issued the Year 2000 Computing Crisis: Business Continuity and Contingency Planning (Exposure Draft) (GAO/AIMD-10.1.19, March 1998).

converted or replaced computer platforms, operating systems, utilities, networks, databases, and interfaces. Moreover, in some instances, agencies may not be able to shut down their production systems for testing and, thus, may have to operate parallel systems implemented at a Year 2000 test facility. Because of the length and complexity of the testing phase and the potential that other test facilities may be needed, our Year 2000 Assessment Guide and DOD's Year 2000 Management Plan recommend that agencies begin identifying the need for test facilities during the assessment phase.

Army Year 2000 Project Office officials acknowledged that they must know the Year 2000 testing requirements of Army components (e.g., equipment, facilities, personnel, and schedule) in order to ensure effective and timely testing of all Army systems. Further, over a year ago, in January 1997, Army Year 2000 Project Office staff recognized that there may be competition for testing resources and agreed to evaluate the issue. However, as of February 1998, the Army Year 2000 Project Office had not yet assessed the situation even though all its mission-critical systems had completed the assessment phase. Without knowing the testing requirements of all Army components, the Army will not be able to effectively schedule resources, prioritize demand, and acquire the additional resources it may need to meet the demands of Year 2000 testing.

Conclusions

The Army's Year 2000 program is at risk of failure because the data required to effectively manage correction efforts are inaccurate and incomplete, interface agreements and contingency plans have not been completed, and all testing requirements have not been determined. In view of these problems, the Army has supplemented its efforts with AAA, the Army Inspector General, and contractor services. However, these initiatives are designed to identify systemic Year 2000 issues and assess the progress made toward resolving them based on data provided, and do not preclude the need for the Army Year 2000 Project Office to effectively and efficiently determine whether system managers are providing complete and accurate information and to ensure that they do. Also, until the Army provides increased oversight of components' efforts to plan for contingencies, prepare interface agreements, and acquire needed testing facilities, it cannot be assured that its mission-critical operations will not be severely degraded or disabled as a result of the Year 2000 problem.

Recommendations

We recommend that the Secretary of the Army direct the Army CIO to do the following:

- Require by July 30, 1998, that all Army components (1) correct their inventory databases, ensuring that they are accurate and complete, (2) certify all claims of Year 2000 compliance and submit completed certification checklists to the Army Year 2000 Project Office, (3) provide reliable Year 2000 cost estimates that are based on a comprehensive inventory and completed assessments of all mission-critical and major systems so that priorities can be established and informed resource trade-off decisions can be made, (4) prepare contingency plans that include specific actions for ensuring the continuity of the Army's critical operations at the Year 2000, (5) prepare memorandums of agreement for all identified interfaces, and (6) develop test plans and identify the need for additional testing resources.
- Require by July 30, 1998, that the Army Year 2000 Project Office ensure that the Army Year 2000 inventory database contains complete, accurate, and current information on Year 2000 status. To accomplish this, the Army Year 2000 Project Office should (1) correct known problems, including erroneous database default values and (2) perform quality assurance checks of the data prior to its use.
- Require that the Army Year 2000 Project Office continuously monitor components' progress in (1) identifying all systems interfaces and defining key details of the data exchange between systems interfaces and (2) preparing and implementing required memorandums of agreement.
- Require that the Army Year 2000 Project Office negotiate with other entities to secure and schedule additional test facilities if components determine that more test capacity is needed.

Agency Comments and Our Evaluation

In written comments on a draft of this report, the Office of the Army Chief Information Officer (CIO) concurred with all of our recommendations and indicated that, based on our review efforts and those of the military audit agencies, actions are already in process to improve the Army Year 2000 program. For example, the CIO noted that, in a February 1998 policy memorandum, he had directed components to (1) provide more complete and accurate data on their systems, (2) ensure that all mission-critical and major systems reported as compliant in the Army Year 2000 database are certified and copies of the certification are provided to the Army Year 2000 Project Office, (3) ensure that all noncompliant mission-critical and major systems are certified following renovation and testing, (4) complete contingency plans for all noncompliant mission-critical and major systems

and core business areas, and (5) inventory all system interfaces and coordinate interface agreements with interface partners. Also, the CIO indicated that he had directed senior-level component managers to meet with him during the April-May 1998 time frame to review progress in fixing Year 2000 issues.

However, as the Army states, many of the actions are not yet complete. Until actions to implement all our recommendations are completed, the Army cannot ensure that it will transition smoothly into the next millennium.

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 sending copies of this letter to the Chairmen and Ranking Minority Members of the Senate Committee on Governmental Affairs and its Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia; 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 Secretary of Defense; the Deputy Secretary of Defense; the Under Secretary of Defense (Acquisition and Technology); the Under Secretary of Defense (Comptroller); the Acting Assistant Secretary of Defense (Command, Control, Communications and Intelligence); the Army's Director of Information Systems for Command, Control, Communications, and Computers; the Commander of the Army Materiel Command; the Army Inspector General; the Army Auditor General; the Director of the Office of Management and Budget; and other interested parties. Copies will be made available to others upon request.

We appreciate the courtesy and cooperation extended to our audit team by Army officials and staff. If you have any questions on matters discussed in this letter, please call me or Ronald B. Bageant, Assistant Director, at (202) 512-6240. Major contributors to this report are listed in appendix III.

Sincerely yours,

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 Army Year 2000 Organizational Structure	22
Appendix II Comments From the Department of the Army	27
Appendix III Major Contributors to This Report	33
Table	Table 1: Reported Status of Army Year 2000 Efforts 8
Figures	Figure I.1: Army Year 2000 Organizational Structure 23 Figure I.2: The Army Materiel Command Organizational Structure 24

Abbreviations

AAA	Army Audit Agency
AMC	Army Materiel Command
CCSS	Commodity Command Standard System
CIO	Chief Information Officer
DISC4	Director of Information Systems for Command, Control, Communications, and Computers
DOD	Department of Defense
LSSC	Logistics Systems Support Center
MACOM	Major Army Command
MOA	memorandum of agreement
OASD/C3I	Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence
OMB	Office of Management and Budget

Army Year 2000 Organizational Structure

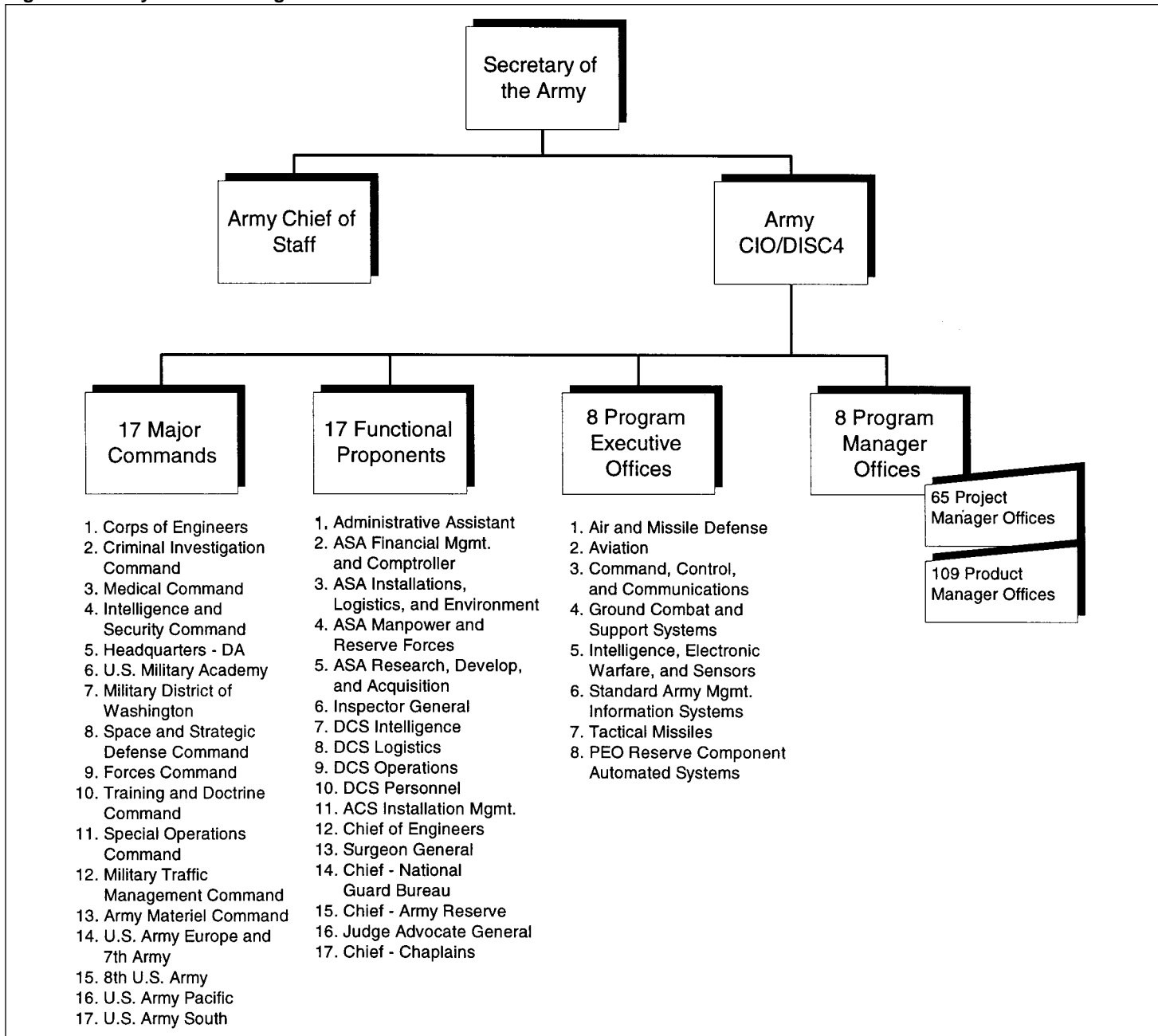
As figure I.1 indicates, Year 2000 management and oversight efforts will have to be coordinated among 17 major commands (MACOM)—each with a complex and diverse organizational structure of its own—17 functional proponents, 8 program executive offices, and 8 program management offices. In addition, 65 project manager offices and 109 product manager offices fall under the MACOM and program executive office umbrellas.

Figure I.2 shows the organizational structure of one major Army command—AMC—in greater detail. To understand the complexity involved in carrying out Year 2000 efforts at the major command level, consider the following information provided by AMC:

- AMC employs more than 65,000 civilian and military employees at 285 locations worldwide.
- The command ranks in business volume with the top 10 corporations in the U.S. and is responsible for about 50 percent of every procurement dollar the Army spends.
- AMC manages about 500,000 computer applications, infrastructure devices, and embedded systems. Of these 500,000,
 - about 476,000 support the business systems infrastructure, such as local area networks and desktop computers and
 - about 1,700 support weapons systems, including the AH-64A Apache and AH-64D Apache Longbow attack helicopters, the M1A2 Abrams tank system and the M2/M3A3 Bradley fighting vehicle, the Patriot missile system, and the Guardrail Common Sensor System used to support the intelligence gathering capabilities of the Army's RC-12 aircraft.
- AMC's 138 logistics business systems include 1,023 system interfaces and 4,694 data bridges.
- AMC has given 149 individuals the responsibility to ensure that Year 2000 problems are resolved.

**Appendix I
Army Year 2000 Organizational Structure**

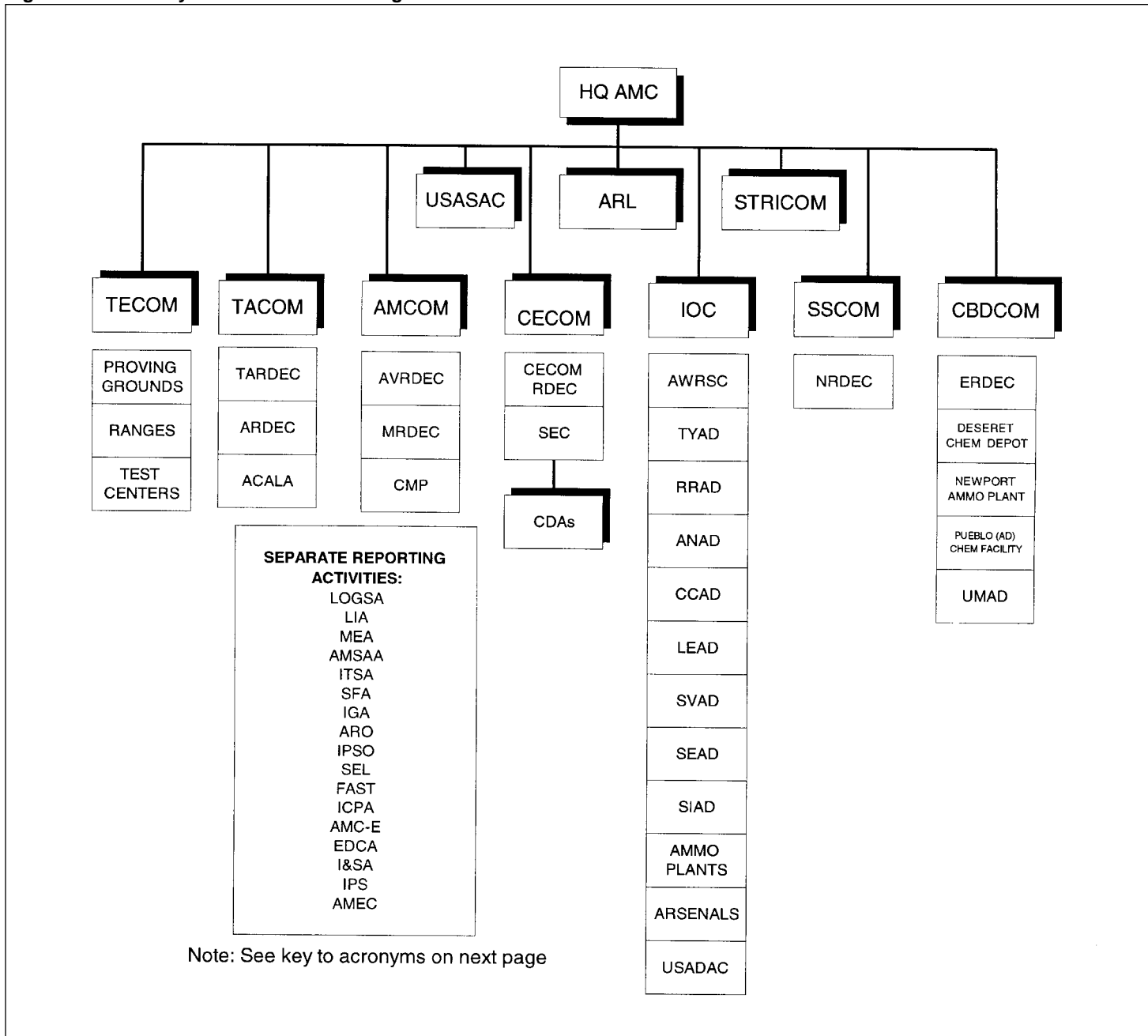
Figure I.1: Army Year 2000 Organizational Structure



Note: The organizational structure depicted above shows only the Army's Year 2000 responsibility and reporting relationships. It does not represent the Army's broader direct command and control environment.

Appendix I
Army Year 2000 Organizational Structure

Figure I.2: The Army Materiel Command Organizational Structure



**The Army Materiel
 Command Organizational
 Structure: Key to
 Acronyms**

Major Subordinate Commands

USASAC	U.S. Army Security Assistance Command
TACOM	U.S. Army Tank-Automotive and Armaments Command
STRICOM	U.S. Simulation, Training and Instrumentation Command
AMCOM	U.S. Army Aviation and Missile Command
CECOM	U.S. Army Communications-Electronics Command
IOC	U.S. Army Industrial Operations Command
ARL	U.S. Army Research Laboratory
SSCOM	U.S. Army Soldier Systems Command
CBDCOM	U.S. Army Chemical and Biological Defense Command
TECOM	U.S. Army Test and Evaluation Command

Activities, Centers, and Depots

TARDEC	Tank-Automotive Research, Development and Engineering Center
ARDEC	Armament Research, Development and Engineering Center
ACALA	Armament and Chemical Acquisition and Logistics Activity
AVRDEC	Aviation Research, Development and Engineering Center
MRDEC	Missile Research, Development and Engineering Center
CMP	Charles Melvin Price Support Center
CECOM RDEC	Communications-Electronics Command Research Development and Engineering Center
SEC	Software Engineering Center
CDAs	Central Design Activities
AWRSC	Army War Reserve Support Command
TYAD	Tobyhanna Army Depot
RRAD	Red River Army Depot
ANAD	Anniston Army Depot
CCAD	Corpus Christi Army Depot
LEAD	Letterkenny Army Depot
SVAD	Savannah Army Depot
SEAD	Seneca Army Depot
SIAD	Sierra Army Depot

(continued)

Appendix I
Army Year 2000 Organizational Structure

USADAC	U.S. Army Defense Ammunition Center
NRDEC	Natick Research, Development and Engineering Center
ERDEC	Edgewood Research, Development and Engineering Center
UMAD	Umatilla Chemical Depot
Separate Reporting Activities	
LOGSA	Logistics Support Activity
LIA	Logistics Integration Activity
MEA	Management Engineering Activity
AMSAA	Army Materiel Systems Analysis Activity
ITSA	Intelligence and Technology Security Activity
SFA	Surety Field Activity
IGA	Inspector General Activity
ARO	Army Research Office
IPSO	Integrated Procurement Systems Office
SEL	School of Engineering and Logistics
FAST	Field Assistance in Science and Technology
ICPA	International Cooperative Programs Activity
AMC-E	Army Materiel Command-Europe
EDCA	Executive Director for Conventional Ammunition
I&SA	Installations and Services Activity
IPS	Integrated Procurement Systems Office
AMEC	Army Management Engineering College

Comments From the Department of the Army

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



Office, Director of Information
Systems for Command, Control,
Communications, & Computers

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

May 6, 1998

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


Dear Mr. Dodaro:

This is the Department of Army response to the General Accounting Office (GAO) draft report, "DEFENSE COMPUTERS: Army Needs to Greatly Strengthen Its Year 2000 Program," dated 25 March 1998 (GAO Code 511628/OSD Case 1572).

The Army has reviewed the draft GAO report and concurs with comments on the recommendations. Technical corrections to the report were separately provided. The detailed comments to the report recommendations are provided in the attachment.

The Army recognizes the Year 2000 (Y2K) issue as a top priority and is taking all prudent steps to ensure that this issue does not pose a threat to our Army's ability to execute its assigned missions prior to, during, and after the Y2K. The Army appreciates the opportunity to comment on the draft report and share with you the actions we have taken and have in process to manage the overall Y2K remediation efforts. The Army primary point of contact for this action is Mr. William Dates, who is my overall Y2K Program Manager, telephone (703) 275-9483.

Sincerely,


WILLIAM H. CAMPBELL
Lieutenant General, GS
Director

Enclosure

Copy Furnished: Department of Defense Office of the Inspector General
Assistant Secretary of Defense for Command, Control and
Communications

Printed on  Recycled Paper

See comment 1.

**GAO DRAFT REPORT - DATED MARCH 25, 1998
(GAO CODE 511628/ OSD CASE 1572)**

**“DEFENSE COMPUTERS: ARMY NEEDS TO
GREATLY STRENGTHEN ITS YEAR 2000 PROGRAM”**

DEPARTMENT OF DEFENSE COMMENTS

RECOMMENDATION 1: The General Accounting Office (GAO) recommended that the Secretary of the Army direct the Army CIO to require all Army components, by 30 July 1998, to (1) correct their inventory databases ensuring that they are accurate and complete, (2) certify all claims of Year 2000 (Y2K) compliance and submit completed certification checklists to the Army Y2K Project Office, (3) provide reliable Y2K cost estimates that are based on a comprehensive inventory and completed assessments of all mission critical and major systems so that priorities can be established and informed resource tradeoff decisions can be made, (4) prepare contingency plans that include specific actions for ensuring the continuity of the Army’s critical operations at the Y2K, (5) prepare memorandums of agreement for all identified interfaces and (6) develop test plans and identify the need for additional testing resources. (p. 30/GAO Draft Report)

DOD RESPONSE: Concur. Partially completed. In process. On 9 February 1998 the Army CIO dispatched a Y2K policy memorandum to the Army major commands and Program Executive Officers (PEOs). This memorandum requires that all mission-critical and major systems that are contained in the Army Y2K database and are coded as compliant be certified and copies of the certification be provided to the Army Y2K Project Office in April 1998. For those systems in the Army database coded as non-

**Appendix II
Comments From the Department of the
Army**

compliant, certification is required following renovation and testing of Y2K fixes. This policy also requires that contingency plans be completed to cover all non-compliant mission critical and major systems in the Army Y2K database not later than 1 June 1998. Interfaces are required to be coordinated with interfacing partners by 1 March 1998. In an effort to have components provide more complete and accurate data on their systems, the Army Y2K Project Office has completed an automated check of existing data records which identifies missing and inconsistent data. These reports have been sent to the appropriate commanders and system proponents in the Army under a cover letter signed by the Army CIO. As part of this review process, the Army CIO is scheduling individual senior level reviews with the commanders, PEOs, and functional proponents in the April-May timeframe to review their progress in fixing Y2K issues.

RECOMMENDATION 2: The GAO recommended that the Secretary of the Army direct the Army CIO to require the Army Y2K Project Office, by 30 July 1998, to ensure that the Army Y2K inventory database contains complete, accurate, and current information on Y2K status. To accomplish this, the Army Y2K Project Office should (1) correct known problems, including erroneous database default values and (2) perform quality assurance checks of the data prior to its use. (pg. 30-31/GAO Draft Report)

DOD RESPONSE: Concur. In process. In order to correct the known default problems with the Army Y2K database and additionally to provide more quality assurance checks of the data, the Army Y2K Project initiated a database redesign effort in September 1997. That effort is nearing completion and a new web-based database will go on line in late

**Appendix II
Comments From the Department of the
Army**

April 1998. This system eliminates the default problems, provides a more user friendly method for data submittal and maintenance, and incorporates, to the maximum extent possible, automatic checks for data integrity and consistency. Additionally, as part of their ongoing audits, the Army Audit Agency is comparing the information in the Army Y2K database with status obtained during their audits and data discrepancies are corrected as they are identified.

RECOMMENDATION 3: The GAO recommended that the Secretary of the Army direct the Army CIO to require the Army Y2K Project Office to continuously monitor components' progress in (1) identifying all systems interfaces and defining key details of the data exchange between systems interfaces and (2) preparing and implementing required memorandums of agreement. (p. 31/GAO Draft Report)

DOD RESPONSE: Concur. In process. Prior to January 1998, the Army Y2K database provided the capability to enter system interface information but not the status of interface memorandums of agreement. This data element has been added and the Army is now tracking this information. Additionally, the Army Audit Agency has been checking on the status and completeness of interface agreements as part of their ongoing audit work in support of the Army Y2K Project Office. In addition to the above actions, the Army is actively participating in the OSD Interface Assessment Workshops which provide us the opportunity to specifically address the status of interfaces by functional area not only among Army systems but with all DOD systems as well. These interface assessment workshops are being held at a rate of 3-4 per month.

RECOMMENDATION 4: The GAO recommended that the Secretary of the Army direct the Army CIO to require the Army Y2K Project Office to negotiate with other entities, including DISA, to secure and schedule additional test facilities should components determine that more test capacity is needed. (p. 31/GAO Draft Report)

DOD RESPONSE: Concur. In process. The Army has been coordinating with DISA to secure and schedule test facilities for Y2K compliance testing through a series of workshops with the applicable central design activities. That process is continuing and no additional test facilities have been identified as being required over and above what DISA is capable of providing. Additionally, in November 1997, the Army Y2K Project Office contracted for an effort on the part of BDM Engineering Services Company to analyze Army Y2K test facility requirements and facility availability to identify any shortfalls so that action could be taken if required. That analysis is scheduled for completion during FY 98. Up to this point, no problems have been surfaced concerning test facility availability in the Army.

Appendix II
Comments From the Department of the
Army

The following is GAO's comment on the Department of the Army's letter dated May 6, 1998.

GAO Comment

1. The Army provided a number of clarifications to the report that we have incorporated as appropriate.

Major Contributors to This Report

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

John B. Stephenson, Senior Advisor
Cristina T. Chaplain, Communications Analyst

Atlanta Field Office

Christopher T. Brannon, Senior Evaluator

Kansas City/St. Louis
Field Office

Denice M. Millett, Evaluator-in-Charge

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

