United States General Accounting Office

GAO

Report to the Acting Director, Defense Finance and Accounting Service

August 1997

DEFENSE COMPUTERS

DFAS Faces Challenges in Solving the Year 2000 Problem

GAO

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

Accounting and Information
Management Division

B-276288

August 11, 1997

Mr. Gary W. Amlin
Acting Director
Defense Finance and Accounting Service

Dear Mr. Amlin:

On June 20, 1997, we briefed members of your staff on the results of our review to date of the Defense Finance and Accounting Service (DFAS) program for solving the 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, DFAS' computer systems could malfunction or produce incorrect information when the year 2000 is encountered during automated data processing. The impact of these failures would be widespread, costly, and potentially debilitating to the DFAS accounting and financial reporting mission.

Our briefing was based on work we performed as part of our review of the Department of Defense's (DOD) Year 2000 computer systems efforts for the Chairman, Senate Committee on Governmental Affairs; the Chairman and Ranking Minority Member of the Subcommittee on Government Management, Information and Technology, House Committee on Government Reform and Oversight; and the Honorable Thomas M. Davis, III, House of Representatives. During the review, we concentrated on determining (1) the status of DFAS' efforts to identify and correct its Year 2000 systems problems and (2) the appropriateness of DFAS' strategy and actions for ensuring that problems will be successfully addressed. This letter summarizes the concerns we raised and provides recommendations for addressing these issues.

Results in Brief

DFAS managers have recognized the importance of solving the Year 2000 problem. If not successfully addressed it could potentially impact DFAS' mission. For example, DFAS systems may be unable to (1) pay millions of active and retired military and civilian personnel and annuitants accurately and on time, (2) disburse funds to pay millions of contractor and vendor invoices, or (3) account for DOD's worldwide operations. To help ensure that services are not disrupted, DFAS has developed a Year 2000 strategy which is based on the generally accepted five-phased government methodology for addressing the Year 2000 problem. This approach is also consistent with our guidelines for planning, managing, and evaluating Year 2000 programs.

In carrying out its Year 2000 strategy, DFAS has assigned accountability for ensuring that Year 2000 efforts are completed, 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. Recently, DFAS also established a Year 2000 certification program that defines the conditions that must be met for automated systems to be considered Year 2000 compliant.

While initial progress has been made, there are several critical issues facing DFAS, that if left unaddressed, may well result in the failure of its systems to successfully operate at the Year 2000. First, DFAS has not identified in its Year 2000 plan all critical tasks for achieving its objectives or established milestones for completing all tasks, specifically the actions that will be needed during the validation (testing) and implementation phases. Second, DFAS has not performed formal risk assessments of all systems to be renovated or ensured that contingency plans are in place in the event that renovations are not completed in time, or if renovated or replacement systems fail to operate properly. Third, DFAS has not identified all system interfaces, including those of external users who have established system connections with DFAS, and has completed written interface agreements with only 230 of 904 interface partners. Fourth, DFAS has not adequately ensured that testing resources will be available when needed to determine if all operational systems are compliant before the year 2000.

DFAS' risk of failure in these areas is increased due to its reliance on other DOD components, such as central design activities, to perform Year 2000 renovations for many of its systems and on the Defense Information Systems Agency (DISA)[1] to ensure that its megacenters can operate in a Year 2000 environment. DFAS is also dependent on military services and DOD components to ensure that their systems are Year 2000 compliant since these entities' systems provide an estimated 80 percent of the financial data that DFAS ultimately uses in its finance and accounting processes. Therefore, it is essential that DFAS take every possible measure

[1] DISA is responsible for DOD information resources management, including the management of data processing facilities and information technology resources at centralized Defense megacenters. DFAS utilizes DISA megacenter computer facilities for processing finance and accounting data and testing changes to information systems.

to ensure that it is well-positioned as it approaches the year 2000 to mitigate these risks and ensure that Defense finance and accounting operations are not disrupted.

Scope and Methodology

During our review, we compared DFAS' efforts to plan and manage its Year 2000 program to our Year 2000 assessment guide for evaluating the awareness and assessment phases. We also performed limited work in areas where DFAS had progressed to the renovation and validation (testing) phases. Specific audit work was performed at DFAS headquarters and three of the five DFAS centers—Cleveland, Denver, and Indianapolis—that, as of April 1997, maintained responsibility over about 83 percent (179 of 216) of the systems that are currently being tracked under the Year 2000 program. Of the 179 systems at these locations, we discussed with system and technical managers the status of 48 systems, about 27 percent of the total. We selected these systems because they cover the three categories of active systems—those to be replaced, those to be renovated, and those already compliant—that DFAS is tracking under its Year 2000 program. Additional factors included consideration of the system size, number of system interfaces, and whether systems were intended to replace existing legacy systems. Appendix I provides a list of the systems that we reviewed.

At DFAS headquarters, we met with the Deputy Director for Information Management, who is responsible for the guidance and direction for the Year 2000 program, to discuss DFAS' strategy for meeting the Year 2000 mandate. We also met with the Year 2000 project manager, who is responsible for the coordination, dissemination, and reporting for the DFAS Year 2000 program, to get an understanding of ongoing activities and requirements. To determine the status of DFAS' contingency planning for automated systems, and its relationship to the Year 2000 program, we obtained DFAS' Corporate Contingency Plan and discussed contingency provisions with officials from the DFAS Plans and Management Deputate and their associates at the DFAS Denver center. We also met with functional managers for six systems DFAS reported as being noncompliant that were the responsibility of the Information Management and Finance Deputates to determine the status of their efforts to achieve Year 2000 compliance.

At the three DFAS centers, we met with individual center directors, who had been given responsibility for ensuring that the systems under their respective centers are Year 2000 compliant. Also, we met with Financial Systems Activity (FSA) Directors, who have technical responsibility for systems maintenance at those locations. We also met with each center's

Year 2000 point of contact who is to disseminate Year 2000 information, and coordinate and consolidate Year 2000 reporting at the center level. Finally, we met with functional and technical managers of 42 separate systems who are being held accountable for ensuring that the systems they are responsible for are Year 2000 compliant.

Using the assessment guide, we reviewed the status of DFAS' Year 2000 awareness by obtaining information on and discussing DFAS' strategy and program management initiatives with top management. We also obtained Year 2000 guidance provided to headquarters and center-level staff, and discussed this guidance with DFAS management responsible for administering the Year 2000 program and ensuring the compliance of DFAS systems.

To determine the extent of assessment and renovation activities being performed, we identified Year 2000 policies and procedures that had been issued, reviewed the status of systems inventories, systems priority processes, risk assessments and contingency planning, and reporting and oversight activities. We interviewed functional and technical managers responsible for specific DFAS systems to discuss the status of their system assessments, the use of assessment tools, and the completeness and reliability of quarterly status report information such as identified milestones, adequacy of resources, interfaces and written agreements, and potential obstacles to meeting Year 2000 compliance. We also discussed with DFAS staff responsible for assessing DFAS' hardware and systems software infrastructure, including its mid-level and communications processors, the status of their efforts to compile an inventory and plan for testing. We also spoke with several systems managers to obtain the status of DFAS' efforts to test and validate commercial-off-the-shelf (COTS) applications.

In evaluating the extent of DFAS' validation phase activities, we met with selected technical managers for six systems classified as compliant to determine the extent of testing that had been performed for asserting compliance. In addition, we tracked the status of DFAS' progress in actually replacing 18 systems that were scheduled to be replaced during a 3-month period. Our audit work was performed from August 1996 through May 1997 using generally accepted government auditing standards.

The Department of Defense provided written comments on a draft of this report. These comments are discussed in the "Agency Comments and Our Evaluation" section and are reprinted in appendix III.

Background

DFAS is the accounting firm of the Department of Defense. It was established in January 1991 to strengthen DOD's financial management operations by standardizing, consolidating, and streamlining finance and accounting policies, procedures, and systems. DFAS accounts for DOD's worldwide operations with assets totalling well in excess of $1 trillion. Each year, DFAS pays nearly 4 million active military and civilian personnel, 2 million retirees and annuitants, and approximately 23 million invoices to contractors and vendors. Due to DFAS' reliance on computer systems to carry out its operations, the Year 2000 issue has the potential to impact virtually every aspect of the DFAS accounting and finance mission. The majority of DFAS finance and accounting systems are 20 or more years old and are primarily written in the Common Business Oriented Language (COBOL) programming language. DFAS recognizes that millions of lines of code must be analyzed and rewritten in systems that will still be operational in the year 2000.

The Year 2000 problem 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 on electronic data storage and reduce operating costs. With this two-digit format, however, the year 2000 is indistinguishable from 1900, or 2001 from 1901. As a result of this ambiguity, system or application programs that use dates to perform calculations, comparisons, or sorting could generate incorrect results when working with years after 1999.

Although DFAS is responsible for the majority of DOD's finance and accounting systems, DFAS is not responsible for all the systems that produce financial data. Systems that support other functional areas such as acquisition, medical, logistics, and personnel originate and process a significant amount of financial data that is ultimately reported on financial statements. These military service and Defense component systems provide financial data to DFAS through systems interfaces that DFAS needs to consider in addressing the Year 2000 problem. The systems that interface with DFAS systems are just as vulnerable to the Year 2000 problem as its own systems. Accordingly, DFAS' ability to sustain operations in the Year 2000 time frame is dependent not only on its own systems, but also on a host of Defense component systems upon which it is largely reliant for accounting transaction data.

In February 1997, we published the Year 2000 Computing Crisis: An Assessment Guide[2] that addresses common issues affecting most federal agencies and presents a structured approach and a checklist to aid them in planning, managing, and evaluating their year 2000 programs. The guide describes five phases—supported by program and project management activities—with each phase representing a major year 2000 program activity or segment. The guidance draws heavily on the work of the Best Practices Subcommittee of the Interagency Year 2000 Committee, and incorporates guidance and practices identified by leading organizations in the information technology industry. The five phases are consistent with those prescribed by DOD in its Year 2000 Management Plan.[3] 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.

In addition to following the five phases described, the Year 2000 program should also be planned and managed as a single large information system development effort. Agencies should promulgate and enforce good management practices on the program and project levels.

[2] Year 2000 Computing Crisis: An Assessment Guide (Exposure Draft) (GAO/AIMD-10.1.14, February 1997).

[3] Department of Defense Year 2000 Management Plan (Version 1.0, April 1997).

Current Status of DFAS Year 2000 Efforts

According to DFAS officials, they have been working on the Year 2000 issue since 1991, although the Year 2000 program did not officially begin until March 1996.[4] As of April 1997, DFAS was tracking 216 systems for Year 2000 purposes: 71 of the 216 were to be renovated to become Year 2000 compliant, 79 were expected to be replaced by migration or interim migration systems, and 66 were designated by DFAS as already compliant.[5] Of the 71 systems DFAS expects to make compliant through renovation, 32 were reported as being in the assessment phase, 36 were in the renovation phase, one was in the implementation phase, and two systems did not show a phase. DFAS has estimated that it will cost $33.7 million to renovate its systems, which contain about 63 million lines of code, to meet Year 2000 requirements.

DFAS has taken a number of positive steps to ensure that its personnel are fully aware of the impact should DFAS finance and accounting systems not be compliant at the turn of the century. During the awareness phase, DFAS developed a Year 2000 strategy that adopts the five-phased approach of awareness, assessment, renovation, validation, and implementation. The strategy, which is embedded in DFAS' written executive plan, establishes accountability for Year 2000 systems compliance from DFAS headquarters management to individual system/program managers at the center level. The Deputy Director for Information Management, who serves as the DFAS Chief Information Officer (CIO), is responsible for managing the Year 2000 program, and overseeing efforts to ensure that all DFAS systems are Year 2000 compliant by December 31, 1998, and within existing funding. As of April 1997, DFAS had taken the following actions as part of its efforts to address the Year 2000 problem:

- established a Year 2000 systems inventory,
- prepared cost estimates for systems to be renovated,
- instituted a quarterly Year 2000 status reporting process,
- appointed a project manager to provide Year 2000 guidance and track Year 2000 progress, and
- established a Year 2000 certification program that defines the conditions that must be met for automated systems to be considered as Year 2000 compliant.

[4] DOD has instituted a decentralized approach whereby individual components are responsible for implementing their own year 2000 programs.

[5] As of April 1997, none of the 66 systems that DFAS reported as being compliant had been validated. As of July 1997, DFAS officials informed us that 9 systems had been certified, however, we did not review these certifications.

DFAS has also performed and documented an analysis of personal computers and workstations, which covered the Year 2000 hardware problems, test procedures and results, and corrective actions. The results of the analysis were provided to DFAS centers for use in testing their hardware. As of April 1997, DFAS reported that over one-third of its nearly 20,000 personal computers had been tested, and that only about 1 percent were found to have been noncompliant. The DFAS Deputy Director for Information Management expects to replace those personal computers that failed the Year 2000 test with compliant computers during the normal equipment upgrade cycles prior to the year 2000.

In addition, DFAS has reported that it has entered its major accounting and financial information systems into DOD's Defense Integration Support Tools (DIST) database. DIST is the database that DOD uses to track its information systems and it is intended to facilitate the Year 2000 effort through its identification of functional systems interfaces and data exchange requirements.[6]

Additional Year 2000 Emphasis and Actions Are Needed

DFAS has taken numerous positive actions during the Year 2000 awareness and assessment phases. However, DFAS is moving forward into renovation, testing, and validation—the more difficult and complex phases of Year 2000 correction—without fully addressing some critical steps associated with the assessment phase. Specifically, DFAS has not

- identified, in its Year 2000 plan, all critical tasks for achieving its objectives or established milestones for completing all tasks,
- performed formal risk assessments of all systems to be renovated and ensured that contingency plans are in place in the event that renovations are not completed in time or if systems fail to operate properly,
- identified all systems interfaces and only a fraction of written interface agreements have been finalized with interface partners, and
- adequately planned to ensure that testing resources are available when needed.

DFAS' risk in these areas is increased due to its dependence on the military services and other Defense agencies, such as DISA, to ensure that their systems and related operating environments are Year 2000 compliant. DFAS will need to work closely with these organizations to ensure that system

[6] DISA acknowledges that, while it has initiated actions to improve the integrity of DIST information, DIST currently is not a reliable and accurate tool for managing the year 2000 effort.

renovations are performed, interface agreements are completed, and proper and timely test environments are provided. If its systems are not operational at the year 2000, DFAS' ability to pay military and civilian personnel, retirees and annuitants, and Defense contractors and vendors could be severely impacted. In turn, DFAS' ability to interact with other DOD components that both provide and use financial data could be jeopardized.

Comprehensive Planning for Year 2000 Program Needed

The Year 2000 program is expected to be the largest and most complex system conversion effort undertaken by federal agencies. Due to the complexities and scope of the Year 2000 problem, it is critical that agencies develop comprehensive plans that establish schedules for all tasks and phases of the Year 2000 program, set reporting requirements, assign conversion or replacement projects to Year 2000 project teams, provide measures for assessing performance, and anticipate the need for risk assessments and contingency plans.

DFAS has issued a high-level Year 2000 executive plan that sets forth its strategy and approach. The plan covers four general areas that DFAS believes will ensure its ability to meet the Year 2000 challenge as follows.

- Ensure that DFAS personnel are aware of the Year 2000 problem by establishing Year 2000 points of contact at multiple organization levels, participating in the DOD Year 2000 Working Group, and distributing Year 2000 information.
- Assess the impact of Year 2000 on DFAS by establishing a systems inventory, replacing systems rather than renovating systems unless impacted prior to replacement, and developing systems as Year 2000 compliant.
- Ensure that DFAS systems are Year 2000 compliant and handle renovations through standard configuration management procedures. Establish responsibility at various levels of the organization—program/system manager, center director and headquarters deputy director, and Deputy Director for Information Management—for achieving Year 2000 compliance.
- Track Year 2000 progress by creating a quarterly consolidated progress report by system that contains information on each system's Year 2000 efforts, such as target implementation date, interface information, and percentage of completion.

Our review of DFAS' Year 2000 plan disclosed that the plan includes a number of positive actions that are consistent with our assessment guide and DOD's management plan. For example, the plan assigns responsibility for achieving Year 2000 compliance, sets forth reporting requirements, and establishes an overall Year 2000 compliance date. However, the plan does not address all phases of the Year 2000 problem, specifically the actions that will be needed during the validation (testing) and implementation phases. The plan also does not establish schedules for completing each phase of the Year 2000 program or milestones for meeting critical tasks under each phase, such as identifying system interfaces and securing interface agreements, preparing contingency plans, defining requirements for and establishing operational Year 2000 compliant test facilities, completing tests of personal computers and servers, or identifying performance measures for evaluating DFAS and center-level progress. DFAS officials have informed us that, while this step is not included in its Year 2000 plan, its system/program managers are now required to have all systems interfaces identified and written interface agreements completed by September 30, 1997, and all personal computers tested by December 31, 1997.

Without comprehensive planning of the Year 2000 project, DFAS runs the risk that it will not have the information to make proper decisions or that necessary tasks will not be addressed in a timely manner. For example, it is important that DFAS establish time frames for completing specific tasks under the Year 2000 program that can be used by DFAS Year 2000 managers as indicators to gauge the progress of individual systems. Equally important is the need to formalize what DFAS managers expect to accomplish during each phase of the Year 2000 effort and within what time frames. For instance, if DFAS system managers have performed system renovations to become Year 2000 compliant, but planning was not conducted early in the process to ensure that adequate test resources or facilities would be available, DFAS runs the risk of systems failure if systems are left untested, or the loss of flexibility to pursue other alternatives before the year 2000.

Greater Emphasis Needed on Assessing Risks and Planning for Contingencies

DFAS has initiated actions to require contingency planning for noncompliant systems that are at risk of not being replaced prior to impact of the year 2000. However, it has not extended its contingency planning to cover systems being renovated as Year 2000 compliant that may not operate at the turn of the century. Contingency plans are important because they identify the alternative activities, which may include manual and contract procedures, to be employed should critical systems fail to meet their Year 2000 deadlines. DOD's Year 2000 Management Plan and our

Year 2000 Assessment Guide call on agencies to initiate realistic contingency plans during the assessment phase for critical systems and activities to ensure the continuity of their core business processes. From an overall agency perspective, DFAS has a Corporate Contingency Plan, which was recently updated in May 1997, that establishes policies, programs, and procedures and assigns responsibilities for the contingency planning process. The plan discusses various possible threats to DFAS activities, but does not specifically address potential year 2000 system failures, nor does it require DFAS managers to include year 2000 failures as part of the updated plan.

DFAS has adopted a strategy for making all systems impacted by the Year 2000 compliant that includes (1) replacing legacy systems with compliant migration or interim migration systems and (2) renovating systems expected to be operational on and after the year 2000. However, DFAS' strategy has two inherent risks. First, because of delays in implementing some migration or interim migration systems, all legacy systems that are expected to be replaced may not be replaced prior to the year 2000. Second, systems being renovated to be compliant may not be completed as scheduled, and renovated systems and those systems DFAS believes to already be compliant, may not correctly operate at the turn of the century. Although DFAS has begun taking steps to address alternative actions if migration systems are delayed, DFAS' overall Year 2000 strategy has not required managers to address alternative actions should systems not operate correctly at the turn of the century. If this latter risk is not addressed and various critical applications fail to operate properly near to or at the turn of the century because of Year 2000 problems, DFAS will encounter interruptions to its accounting and financial activities with no clear alternative actions to help ensure continuity of operations.

DFAS Has Begun Planning for Contingencies Should Legacy Systems Not Be Replaced

DFAS is relying on the success of the DOD migration program to solve a significant portion of its Year 2000 problem. DFAS' April 1997 quarterly status report indicates that about 80 existing legacy systems are to be replaced with 27 interim migration and migration systems, and several COTS systems. The DOD migration program, however, has a long history of problems,[7] including missed milestones. Our current work has shown that many of DFAS' legacy systems had not been replaced according to projected plans. Also, in some instances, replacement decisions had not

[7] Our reports Defense IRM: Critical Risks Facing New Materiel Management Strategy (GAO/AIMD-96-109, September 6, 1996) and Defense IRM: Strategy Needed for Logistics Information Technology Improvement Efforts (GAO/AIMD-97-6, November 14, 1996), among others, point out numerous weaknesses in Defense's migration strategy that impacted the timely development of replacement systems and the legacy systems they were to replace.

been finalized because of concerns over incorporating the legacy system requirements into the migration or interim migration systems.

To assess the likelihood that systems already scheduled to be replaced would be replaced as planned, we identified 18 systems from DFAS' October 1996 Year 2000 quarterly report that were scheduled for replacement or termination by January 1997 (see appendix II for the number of systems not replaced or terminated by location). Of those 18 systems, we found that 11 had not been replaced or terminated as planned. While these systems could incur additional slippage and still be replaced before being impacted by the Year 2000 problem, DFAS' ability to meet tight deadlines for replacing systems may well become more difficult as the need for technical staff and resources increase for Year 2000 activities.

One example of this problem is the deployment of the Standard Accounting and Reporting System (STARS). STARS is a DFAS interim migration system intended to replace eight noncompliant legacy accounting systems before the year 2000. In September 1996,[8] we reported that the STARS migration project had experienced a number of problems over the years, including incomplete planning, missed milestones, and budget overruns. One specific system that was to have been replaced by STARS in January 1997 is the Naval Civilian Engineering Laboratory Financial Management Data System (NCEL-FMDS). However, as of April 1997, DFAS reported that NCEL-FMDS would be replaced by a COTS system by August 1997. Another system—the U.S. Naval Academy Trust Fund Accounting System (NTFAS)[9]—was to have been replaced by STARS as of December 1996. While the April 1997 DFAS Year 2000 quarterly status report shows that a date for replacing NTFAS with STARS had yet to be determined, recent discussions with DFAS personnel indicate that NTFAS had been terminated. At the time of our report, DFAS had not provided documentation to support this assertion.

DFAS recognizes the concern that some migration and interim migration systems may be delayed, and has begun actions to renovate some legacy systems that were originally designated for replacement. DFAS has also required its systems managers, for all systems to be replaced, to assess and report the risk—using a high-; medium-; or low-risk designation—of

[8] DOD Accounting Systems: Efforts to Improve System for Navy Need Overall Structure (GAO/AIMD-96-99, September 30, 1996).

[9] According to DFAS, NCEL-FMDS and NTFAS are Navy systems that are being monitored by DFAS because they are sources of financial information and because they were scheduled to be replaced by STARS—a DFAS interim migration system.

their systems not being replaced prior to being impacted by Year 2000 problems. Systems managers for all systems to be replaced that were designated as having a high or medium risk are to have prepared plans identifying how they intend to fix the Year 2000 problem. Beginning in July 1997, DFAS reports that it intends to start monitoring the existence of these systems plans through its quarterly reporting process. Further, DFAS also intends to begin tracking other information that should help it make decisions as to whether to renovate, or take other alternative actions, for additional legacy systems that are now expected to be replaced. For example, systems managers will be required to report the latest possible start date to initiate a system renovation that would still allow them to meet the compliance deadline. This requirement calls for having contingency plans in place for over 80 percent of the systems to be replaced. However, because of the uncertainty associated with the implementation of DFAS' migration systems, potentially there are still gaps that may necessitate DFAS extending this requirement to all systems scheduled to be replaced that support critical operations or provide data to those systems.

Potential Operational Failures Need to Be Better Addressed

The year 2000 represents a great potential for operational failure to DFAS that could adversely impact its core business processes as well as those of entities that depend on DFAS for accounting and financial reporting. To mitigate this risk of failure, our assessment guide and DOD's management plan suggest that agencies perform risk assessments and prepare realistic contingency plans that identify alternatives to ensure the continuity of core business processes in the event of a failure. These alternatives could include performing automated functions manually or using the processing services of contractors. While DFAS managers have begun preparing contingency plans for legacy systems that may not be replaced by compliant systems prior to the year 2000, the DFAS Year 2000 strategy does not require managers to assess risk, or plan for contingencies, if systems being renovated fail to operate at the year 2000. Also, the recently updated DFAS Corporate Contingency Plan does not require managers to address contingencies for a potential Year 2000 failure. DFAS needs this protection to ensure that, in the event of an operational failure, major functional activities are not disrupted at the year 2000.

DFAS currently has identified 71 systems that it plans to make compliant through renovation, and an additional 66 systems that are reported as being compliant, but have not yet been fully tested in a Year 2000 operating environment. Although the DFAS Year 2000 program calls for these systems to eventually be validated prior to implementation, even with a structured process for assessing systems' compliance, DFAS systems are still at risk that unanticipated operational failure could occur. In addition, DFAS systems interact with many DOD component and military service systems, and as a result, an operational failure in one system or process would not only impact functions these systems currently perform but could also impact other related activities. Because many of the continuity of operation alternatives that traditionally apply to threats, such as back-up processing sites, cannot be relied upon to address Year 2000 issues, it is important that DFAS' functional and technical managers have policies and procedures in place to ensure that critical activities can be performed in the event of system failure. The absence of good contingency planning increases DFAS' risk that its operations could be disrupted.

System Interfaces Present Challenges

The success of DFAS finance and accounting operations hinges on the proper and timely exchange of data with others. DFAS systems interface internally with hundreds of other DFAS systems and externally with military services, Defense components, and various federal government systems. DFAS receives an estimated 80 percent of the data it uses in its finance and accounting processes from non-DFAS systems. It is critically important during the Year 2000 effort that agencies protect against the potential for introducing and propagating errors from one organization to another and ensure that interfacing systems have the ability to exchange data through the transition period. This potential problem may be mitigated through formal agreements between interface partners that describe the method of interface and assign responsibility for accommodating the exchange of data. DOD's Year 2000 Management Plan places responsibility on component heads or their designated Year 2000 points of contact to document and obtain system interface agreements in the form of memorandums of agreement (MOA) or the equivalent.

DFAS' Year 2000 strategy calls for its system managers to identify interfaces for all systems that are to be renovated for Year 2000 compliance and to obtain written MOAS between interface partners. System managers also are required to identify the number of internal and external systems interfaces[10] and the number of interfaces that are covered by MOAS and include this as part of the DFAS Year 2000 quarterly reporting process. The number of interfaces not impacted by the Year 2000 problem are also reported separately for each system.

[10] An internal interface transfers data between two DFAS-owned systems, whereas an external interface transfers data between a DFAS-owned and a non-DFAS-owned system.

As of April 1997, DFAS reported that system/program managers had identified 904 internal and external interfaces that are affected by the year 2000 problem, although managers still had not identified all interfaces. Of the 904 system interfaces that had been identified, 451 were reported as internal interfaces and 453 were identified as external interfaces. According to DFAS, written MOAS, covering how and when the interfaces are to be accomplished, had been completed for only 230 of the system interfaces. DFAS' quarterly report shows that significantly less progress has been made in securing written MOAS for external system interfaces than for those internal to DFAS. Of the 230 completed MOAS, only 82 were with external interface partners. DFAS officials have set September 30, 1997, as the deadline for securing all MOAS, both internal and external, with interface partners.

While the number of interfaces is a major Year 2000 concern to DFAS, the importance and complexity of the interface issue is compounded due to DFAS' use of different strategies[11] for making systems Year 2000 compliant. DFAS reports that about one-third of the systems it plans to renovate are using procedural code[12] or sliding windows[13] as the predominate strategies for becoming Year 2000 compliant. As such, the use of different strategies in systems that exchange data through interfaces may require the use of bridging.[14] With these strategies, each interface partner will have to clearly understand the logical date interpretations that each is using to ensure that the appropriate century is applied when exchanging two-digit year data. Additional monitoring and oversight may be necessary to ensure that compliant date strategies that depend on date logic are implemented correctly.

Timely and complete information on all system interfaces that may be affected by Year 2000 changes is critical to the success of DFAS' Year 2000 compliance program. The amount of work required to coordinate the data

[11] DOD has identified three strategies—field expansion, procedural code, and sliding windows—for purposes of renovating noncompliant systems. Field expansion increases the size of the date field generally from a two-digit year to a four-digit year. Procedural code and sliding windows derive the correct century based on the two-digit year.

[12] Procedural code is code which 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).

[13] Sliding windows are similar to procedural code in that they 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.

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

being exchanged between systems must be known as early as possible, and documented in written MOAS, in order that DFAS may complete maintenance schedules, allocate resources, plan testing, and schedule implementation.

Additional Focus Needed on Systems Testing

We expect that agencies may need over a year to adequately validate and test converted or replaced systems for Year 2000 compliance, and that the testing and validation process may consume over half of the Year 2000 program resources and budget. While DFAS technical managers have performed certain Year 2000 tests of individual systems as part of their normal software maintenance processes, DFAS has not yet performed sufficient planning to ensure that all necessary testing will be conducted prior to Year 2000 impact. Also, some systems that DFAS has designated as already compliant had not been fully tested to support that assertion. Our 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. During the assessment phase, DFAS had not yet developed test plans for all systems it plans to have operational at the year 2000, including those systems to be renovated and those already classified as compliant. DFAS also had not yet defined what Year 2000 test facilities it expected to use and ensured their availability.

Much of DFAS' testing is dependent upon others to provide the needed assurances that systems are Year 2000 compliant. For example, about 40 percent of DFAS' systems are technically maintained by central design activities (CDAS) that are managed by another Defense component or a military service. These activities are likely to have differing processes for conducting system testing. Also, before DFAS managers can be assured that systems under their responsibility are compliant, the systems will need to be tested in an operating environment using a Year 2000 compliant operating system. DISA is responsible for providing a Year 2000 compliant operating environment and resources for testing systems, including many DFAS systems, at DISA megacenters. DFAS will also need assurances from vendors that its COTS applications are Year 2000 compliant. While DFAS' recent establishment of a certification program should provide additional assurance that systems have been tested, the program will need to be properly implemented at all locations. Without planning for the proper and timely testing of all systems, DFAS runs the risk of potential contamination to systems data or interference with the operation of production systems.

Systems Asserted as Compliant Have Not Been Fully Tested

On the basis of our analysis, we found that DFAS had not performed adequate testing to assert that its compliant systems are capable of transitioning into the year 2000. According to the DFAS April 1997 quarterly status report, 66 of its 216 systems tracked for Year 2000 purposes are classified as compliant. DFAS' compliant systems can be grouped into four categories: already converted, not date sensitive, under development, and compliant COTS products. To determine if DFAS had a sufficient basis for asserting Year 2000 compliance, we selected six systems that DFAS had designated as compliant and reviewed supporting documentation provided by technical managers for three of the six that were identified as already converted. The remaining three systems were either in the process of being developed Year 2000 compliant or deemed to not be date sensitive. Managers of the already converted, compliant systems we spoke with indicated that they had performed some tests on the transfer and storage of dates, but had not completed all Year 2000 compliance tests. For example:

- A technical manager for the Defense Transportation Pay System (DTRS) stated that system integration tests[15] to input four-digit year data from a keyboard entry and from an electronic entry had been performed. However, system acceptance tests[16] to determine Year 2000 compliance had not been performed at the time of our review.
- A technical manager for another compliant system—the Uniform Microcomputer Disbursing System (UMIDS)—indicated that the system had already been converted to accommodate the year 2000, and that some testing had been performed. All systems tests, however, including those to determine if UMIDS could operate in a Year 2000 environment with its interfaces, were not scheduled to be completed until fall 1997.
- A technical manager of another system reported as compliant—the Standard Army Financial Inventory Accounting and Reporting System-MOD (STARFIARS-MOD)—stated that this system could not be completely tested until a Year 2000 compliant compiler for Ada[17] was available.

On April 11, 1997, the DFAS Deputy Director for Information Management issued guidance for establishing a Year 2000 automated information

[15] System integration tests are designed to determine if related information system components perform to specification, such as verifying that computer programs operate with equipment, subsystems, and other systems.

[16] System acceptance tests are formal tests designed to determine whether or not the software end product is valid and represents what was specified by the customer.

[17] Ada is a powerful software programming language that was developed under DOD's sponsorship and used extensively in many of its systems.

system certification program. The intent of the certification program is to define conditions, through completion of a certification checklist, that must be met in order that systems can be considered as Year 2000 compliant.[18] Under the certification program, systems identified in DFAS' Year 2000 quarterly status report as to be renovated, being developed compliant, and compliant, are to be certified. System/program managers are to complete the certification no later than 1 month after a system acceptance test is performed and the system is deemed compliant. The certification checklist requires signatures of the technical manager responsible for performing system changes, the system/program manager responsible for ensuring that the system is compliant, and the center director or headquarters deputy director responsible for Year 2000 compliance of all systems at their respective locations.

Because the certification program had only recently been established, we were unable to assess to what extent it had been implemented, and therefore, how well the process was working. If implemented effectively and consistently, the process should provide DFAS a more reliable basis for asserting compliance of its systems.

Systems Still Need To Be Tested With Compliant Operating System

DFAS systems have not been tested for their ability to operate in a compliant Year 2000 environment because DISA has not installed Year 2000 compliant operating systems. DISA plans to upgrade its large-scale IBM and Unisys operating systems to be Year 2000 compliant over the next 2 years. For example, DISA and DFAS plan to incrementally implement the new IBM OS/390 operating system and make necessary conversions to existing applications from April 1997 to October 1998. Once implementation is completed for a particular domain, system testing can begin. About 45 DFAS systems, many of which are processed on mainframes, are classified as already converted, compliant, or not date sensitive, but still need to be tested to ensure that they do not encounter problems with the new operating system.

No Process for Ensuring COTS Compliance

DFAS has not defined a validation process for ensuring that its COTS applications are Year 2000 compliant. Since most suppliers of COTS software do not disclose their source code or the internal logic of their products, testing should be complemented by a careful review of warranties and/or guarantees. At the time of our review, DFAS had not

[18] As of June 19, 1997, DFAS updated its certification program to include two certification levels. Certification level 1 is an interim certification where a system may be considered to be compliant, but one or more of its interface agreements may not be completed. In order to meet certification level 2, a system must be fully compliant and be operating in accordance with interface agreements. For systems to achieve both certification levels, all necessary systems testing must be completed.

required the testing of COTS applications that are being reported as compliant. Although systems managers had been given responsibility for obtaining written assurances from their vendors that COTS products are compliant, no documentation had been obtained to provide these assurances. Without an effective validation process for assuring COTS Year 2000 compliance, DFAS runs the risk that these applications will not operate correctly in the future.

Conclusions

While initial progress has been made, there are several critical issues facing DFAS, that if left unaddressed, may well result in the failure of its systems to operate at the year 2000. As the accounting arm of DOD, DFAS has a responsibility to its customers to ensure that its systems support their needs and produce accurate, reliable, and timely financial information on the results of DOD's operations. At the same time, its operations hinge on the ability of systems belonging to the military services and other components to be Year 2000 compliant. Additionally, DFAS is dependent on numerous central design activities that are not under its control to perform Year 2000 renovations to many of its systems. Although DFAS managers have recognized the importance of solving Year 2000 problems in their systems, to reduce the risk of failure with its own Year 2000 effort, it is critically important that DFAS take every measure possible to ensure that it is well-positioned to deal with unexpected problems and delays. This includes promptly implementing Year 2000 project and contingency planning as well as addressing critical systems interfacing and testing issues.

Recommendations

We recommend that you direct the DFAS Deputy Director for Information Management to:

- Build upon the existing DFAS project plan to ensure that it identifies the actions and establishes the schedules for completing each phase of the Year 2000 program, including the validation (testing) and implementation phases. The plan should also identify the milestones for meeting critical tasks under each phase, such as identifying system interfaces and securing interface agreements, preparing contingency plans, defining requirements for and establishing operational Year 2000 compliant test facilities, completing tests of personal computers and servers, and identifying performance measures for evaluating DFAS and center-level progress.
- Ensure that DFAS' Corporate Contingency Plan addresses the Year 2000 crisis and provides guidance for ensuring continuity of operations. The

guidance should require DFAS managers to perform risk assessments and prepare contingency plans for all critical systems impacted by the year 2000 and for all noncritical systems impacted by the year 2000 that provide data to critical systems. Specifically, risk assessments and contingency plans should be required for all critical systems, including the identification of alternatives in the event that (1) replacement systems are not available, (2) systems to be renovated are not completed, and (3) systems fail to operate as intended prior to Year 2000 impact.

- Require the timely identification of all internal and external systems interfaces and the completion of signed, written interface agreements that describe the method of data exchange between interfacing systems, the entity responsible for performing the system interface modification, and milestones identifying when the modification is to be completed.
- Require the full implementation of the recently established Year 2000 certification process and ensure that Year 2000 compliance is predicated on testing all systems, including COTS applications and personal computers and servers.
- Devise a testing schedule that identifies the test facilities and resources needed for performing proper testing of DFAS systems to ensure that all systems can operate in a Year 2000 environment.

Agency Comments and Our Evaluation

In written comments on a draft of this report, the Office of the Under Secretary of Defense (Comptroller) concurred with all of our recommendations to improve the DFAS Year 2000 program. In response to our recommendations, DFAS agreed to update its existing Year 2000 Executive Plan to ensure that it identifies the actions and establishes the schedules for completing each phase of the Year 2000 program, including the validation (testing) and implementation phases, and the milestones for meeting critical tasks under each phase. DFAS also agreed to update its Corporate Contingency Plan to require a risk assessment and business impact analysis of all mission critical systems and critical direct support systems for the Year 2000 crisis, including the addition of requirements to test critical systems for Year 2000 compliance and to identify contingency strategies for dealing with noncompliant situations.

In addition, DFAS agreed to have all written interface agreements with interface partners in place by September 30, 1997, and to implement its Year 2000 certification process for ensuring all systems are compliant. Further, DFAS agreed to develop a testing schedule that identified the test facilities and resources needed for performing proper testing of DFAS systems to ensure those systems can operate in a Year 2000 environment.

DFAS pointed out that it is working closely with DISA to coordinate the implementation of the Year 2000 environment, since DFAS is dependent on DISA to actually install and operate that environment. The full text of DOD's comments are provided in appendix III.

This report contains recommendations to you. Within 60 days of the date of this report, we would appreciate receiving a written statement on actions taken to address these recommendations.

We appreciate the courtesy and cooperation extended to our audit team by DFAS officials and staff. We are providing copies of this letter to the Chairman and Ranking Minority Member of the Senate Committee on Governmental Affairs; 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, and the Subcommittee on Government Management, Information and Technology, House Committee on Government Reform and Oversight; the Honorable Thomas M. Davis, III, House of Representatives; the Deputy Secretary of Defense; the Acting Under Secretary of Defense (Comptroller); the Assistant Secretary of Defense (Command, Control, Communications and Intelligence); the Director of the Office of Management and Budget; and other interested parties. Copies will be made available to others upon request.

If you have any questions on matters discussed in this letter, please call me at (202) 512-6240 or Ronald B. Bageant, Assistant Director, at (202) 512-9498. Major contributors to this report are listed in appendix IV.

Sincerely yours,

Jack L. Brock, Jr.
Director, Defense Information and
Financial Management Systems

Contents

Abbreviations

CDA	central design activities
CIO	Chief Information Officer
COBOL	Common Business Oriented Language
COTS	commercial-off-the-shelf
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DIST	Defense Integration Support Tools
DOD	Department of Defense
DTRS	Defense Transportation Pay System
FSA	Financial Systems Activity
IBM	International Business Machines, Inc.
MOA	Memorandums of Agreement
NCEL-FMDS	Naval Civilian Engineering Laboratory Financial Management Data System
NTFAS	U.S. Naval Academy Trust Fund Accounting System
STARFIARS-MOD	Standard Army Financial Inventory Accounting and Reporting System-MOD
STARS	Standard Accounting and Reporting System
UMIDS	Uniform Microcomputer Disbursing System

DFAS Systems Reviewed

	Organization acronym - name	System classification	Year 2000 phase as of January 1997	Lines of code
	DFAS- Headquarters			
1	DCPS - Defense Civilian Pay System	To be renovated	Renovation	944,000
2	DJMS-AC - Defense Joint Military Pay System-Active Component	To be renovated	Renovation	5,134,069
3	DJMS-RC - Defense Joint Military Pay System-Reserve Component	To be renovated	Renovation	1,211,947
4	MCTFS - Marine Corps Total Force System	To be renovated	Renovation	2,532,973
5	DFAS Order Writer	To be replaced	N/A	58,556
6	CMIS - Configuration Management Information System	To be renovated (reengineering)	Renovation	223,744
	DFAS-Indianapolis			
7	HQARS - Headquarters Accounting and Reporting System	To be replaced	N/A	1,710,000
8	SOMARDS - Standard Operations and Maintenance, Army R&D System	To be renovated	Assessment	950,000
9	SIFS - Standard Industrial Fund System	To be renovated	Renovation	3,400,000
10	NAFCPS - Non-appropriated Funds Civilian Payroll System	To be renovated	Assessment	305,000
11	NAFISS - Non-appropriated Funds Information Standard System	To be replaced	N/A	200,000
12	CEFMS - Corps of Engineers Financial Management System	To be renovated (reengineering)	Assessment	2,250,000
13	PBAS-FD - Program and Budget Accounting System - Fund Distribution	To be renovated	Assessment	1,600,000
14	STARFIARS-MOD - Standard Army Financial Inventory Accounting and Reporting System - MOD	Compliant	N/A	840,000
15	SRD-1 - Standard Finance System -Redesign (Subsystem 1)	To be renovated	Renovation	1,800,000
16	COA Host - Controller of the Army Host	To be replaced	Terminated	9,272,500
17	EDMS - Electronic Document Management System - Loss and Damage	To be renovated	Assessment	40,000
18	ADARS - Automated Drill Attendance Reporting System	To be replaced	Transferred to Army	N/R
19	JUSTIS - Jumps Terminal Input System	To be replaced	Transferred to Army	N/R
20	TAXMRI - Tax Machine Readable Input	To be replaced	N/A	N/R
21	UCS - Unemployment Compensation System	Compliant	N/A	N/R
22	DTRS - Defense Transportation Pay System	Compliant	N/A	360,000
23	TD&RS - Transportation Disbursing and Reporting System	To be replaced	N/A	156,000

(continued)

	Organization acronym - name	System classification	Year 2000 phase as of January 1997	Lines of code
24	STARFIARS - Standard Army Financial Inventory Accounting and Reporting System	To be replaced	N/A	200,500
25	CAPS - Computerized Accounts Payable System	To be renovated (reengineering)	Renovation	57,000
26	STARCIPS - Standard Army Civilian Payroll System	To be replaced	N/A	208,430
27	SNIPS - Standard Negotiable Instrument Processing System	To be replaced	N/A	118,000
28	CRISPS - Consolidated Return Items Stop Payment System	To be replaced	N/A	57,000
29	STANFINS - Standard Financial System	To be renovated	Assessment	675,000
30	TUFMIS - Tactical Unit Financial Management Information System	To be replaced	N/A	35,000
	DFAS-Denver:			
31	DIFS - Defense Integrated Financial System	To be renovated	Assessment	1,843,041
32	CMCS - Case Management Control System - Accounting Segment	To be renovated	Assessment	1,833,748
33	GAFS - General Accounting and Finance System - Base Level	To be renovated	Assessment	975,000
34	SMAS - Standard Material Accounting System	To be renovated	Assessment	1,300,000
35	DRAS-APS - Defense Retiree and Annuitant Pay System - Annuitant	To be renovated	Renovation	921,751
36	SOF - Status of Funds System	To be renovated	Assessment	321,000
37	DCMS - Departmental Cash Management System	Compliant - being developed	N/A	N/R
38	MAFR - Merged Accountability and Fund Reporting System	To be replaced	N/A	262,316
	DFAS-Cleveland			
39	NIFMS - NAVAIR Industrial Financial Management System	To be renovated	Renovation	2,568,018
40	FCS China Lake	To be replaced	N/A	3,000,000
41	STARS - Standard Accounting and Reporting System	To be renovated	Assessment	3,706,000 + new development
42	DFRRS - Departmental Financial Reporting and Reconciliation System	Compliant - being developed	N/A	N/R
43	SYMIS - Shipyard Management Information System	To be renovated	Assessment	1,733,000
44	RIMS - Real Time Integrated Management System	To be renovated	Assessment	3,300,000
45	NRDPS - Naval Reserve Drill Pay System	To be replaced	N/A	231,000

(continued)

	Organization acronym - name	System classification	Year 2000 phase as of January 1997	Lines of code
46	UMIDS - Uniform Microcomputer Disbursing System	Compliant	N/A	430,000
47	DRAS-RCP - Defense Retiree and Annuitant Pay System - Retiree	To be renovated	Renovation	743,000
48	NJUMPS - Navy Joint Uniform Military Pay System	To be replaced	N/A	1,250,000
	Totals			

	Headquarters = 6
	Indianapolis = 24
	Denver = 8
	Cleveland = 10
	Total = 48
		To be renovated= 25
		To be replaced = 17
		Compliant = 6
		Total = 48
			Assessment = 14
			Renovation = 11
			Total = 25
				< than 1 m= 24
				1 m to 3 m=12
				> than 3 m = 6
				Unknown = 6
				Total = 48

Note: N/A = Not applicable; N/R = Not reported

Source: DFAS Year 2000 Quarterly Status Report as of January 10, 1997.

DFAS Systems That Were Not Replaced or Terminated as Scheduled in January 1997

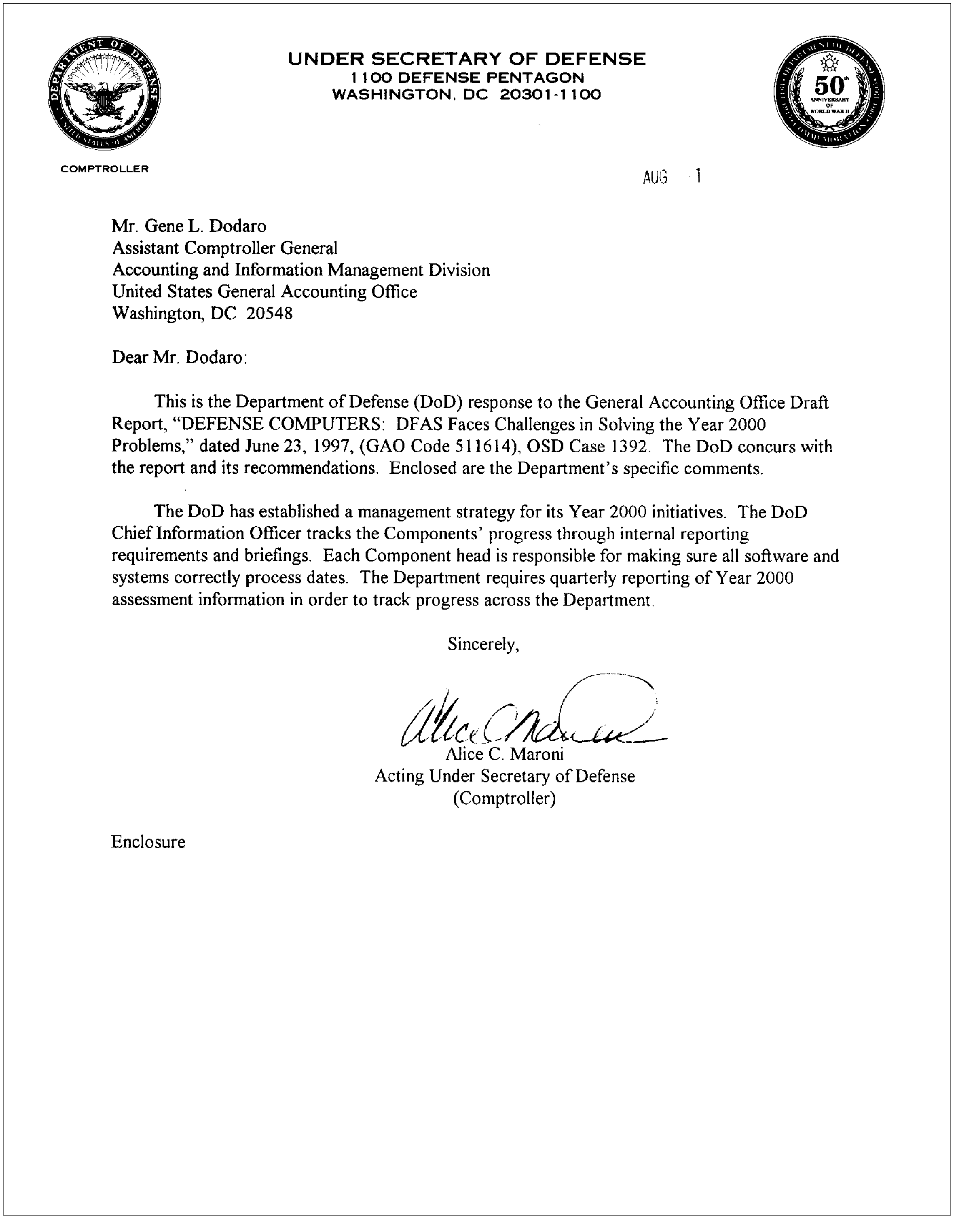
DFAS Center	Systems that were to be replaced or terminated as of January 1997	Systems that were not replaced or terminated as of January 1997
Cleveland (CL)	13	8
Indianapolis (IN)	3	2
Kansas City (KC)	2	1
Totals	**18**	**11**

Note: The October 1996 DFAS Year 2000 Quarterly Status Report did not list any systems to be terminated or replaced by January 1997 for DFAS-Headquarters, DFAS-Columbus, and DFAS-Denver.

Source: DFAS Year 2000 quarterly status reports for October 1996 and January 1997.

Appendix III

Comments From the Department of Defense



UNDER SECRETARY OF DEFENSE
1100 DEFENSE PENTAGON
WASHINGTON, DC 20301-1100

COMPTROLLER

AUG 1

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

Dear Mr. Dodaro:

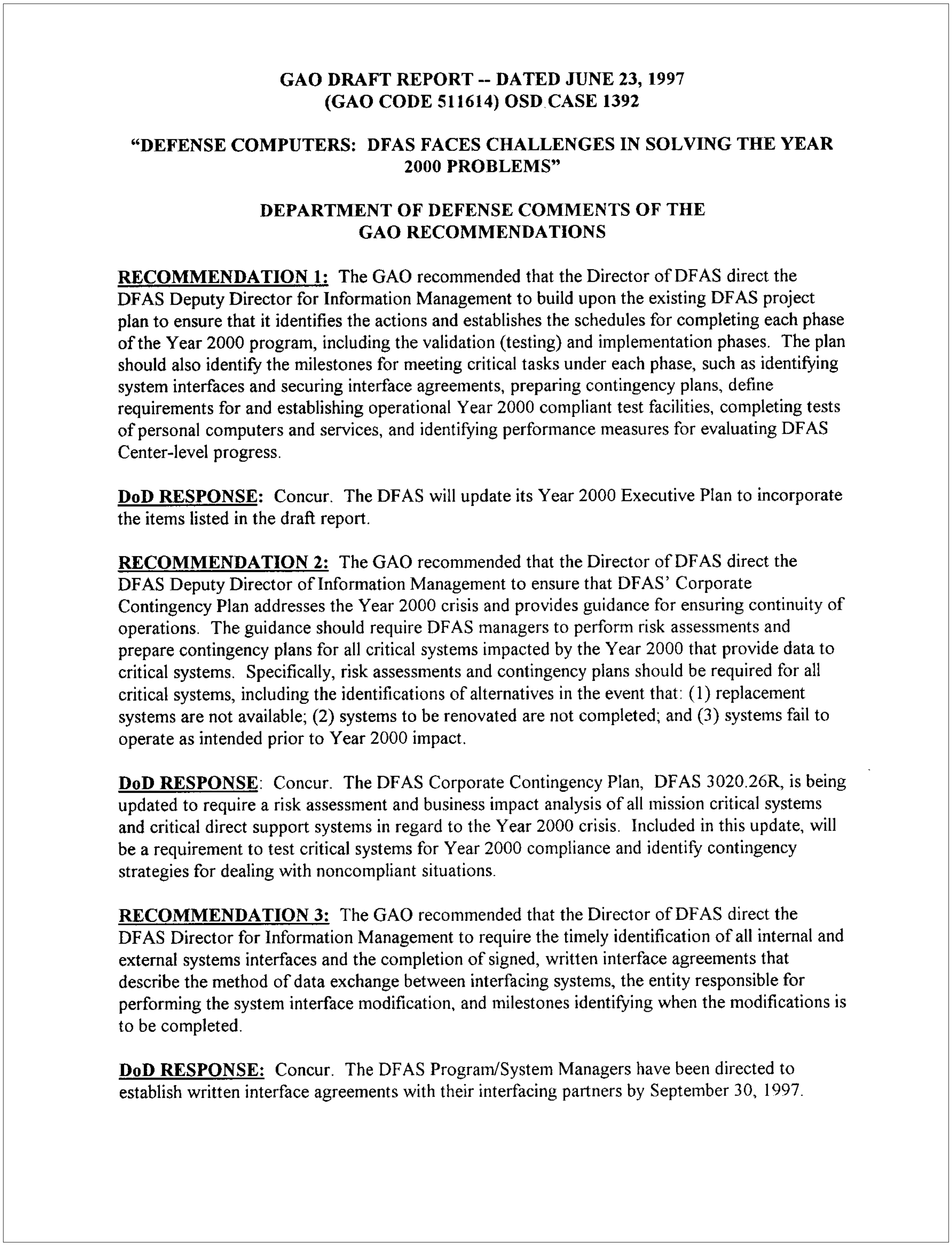
This is the Department of Defense (DoD) response to the General Accounting Office Draft Report, "DEFENSE COMPUTERS: DFAS Faces Challenges in Solving the Year 2000 Problems," dated June 23, 1997, (GAO Code 511614), OSD Case 1392. The DoD concurs with the report and its recommendations. Enclosed are the Department's specific comments.

The DoD has established a management strategy for its Year 2000 initiatives. The DoD Chief Information Officer tracks the Components' progress through internal reporting requirements and briefings. Each Component head is responsible for making sure all software and systems correctly process dates. The Department requires quarterly reporting of Year 2000 assessment information in order to track progress across the Department.

Sincerely,

Alice C. Maroni
Acting Under Secretary of Defense
(Comptroller)

Enclosure



GAO DRAFT REPORT -- DATED JUNE 23, 1997
(GAO CODE 511614) OSD CASE 1392

"DEFENSE COMPUTERS: DFAS FACES CHALLENGES IN SOLVING THE YEAR 2000 PROBLEMS"

DEPARTMENT OF DEFENSE COMMENTS OF THE
GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommended that the Director of DFAS direct the DFAS Deputy Director for Information Management to build upon the existing DFAS project plan to ensure that it identifies the actions and establishes the schedules for completing each phase of the Year 2000 program, including the validation (testing) and implementation phases. The plan should also identify the milestones for meeting critical tasks under each phase, such as identifying system interfaces and securing interface agreements, preparing contingency plans, define requirements for and establishing operational Year 2000 compliant test facilities, completing tests of personal computers and services, and identifying performance measures for evaluating DFAS Center-level progress.

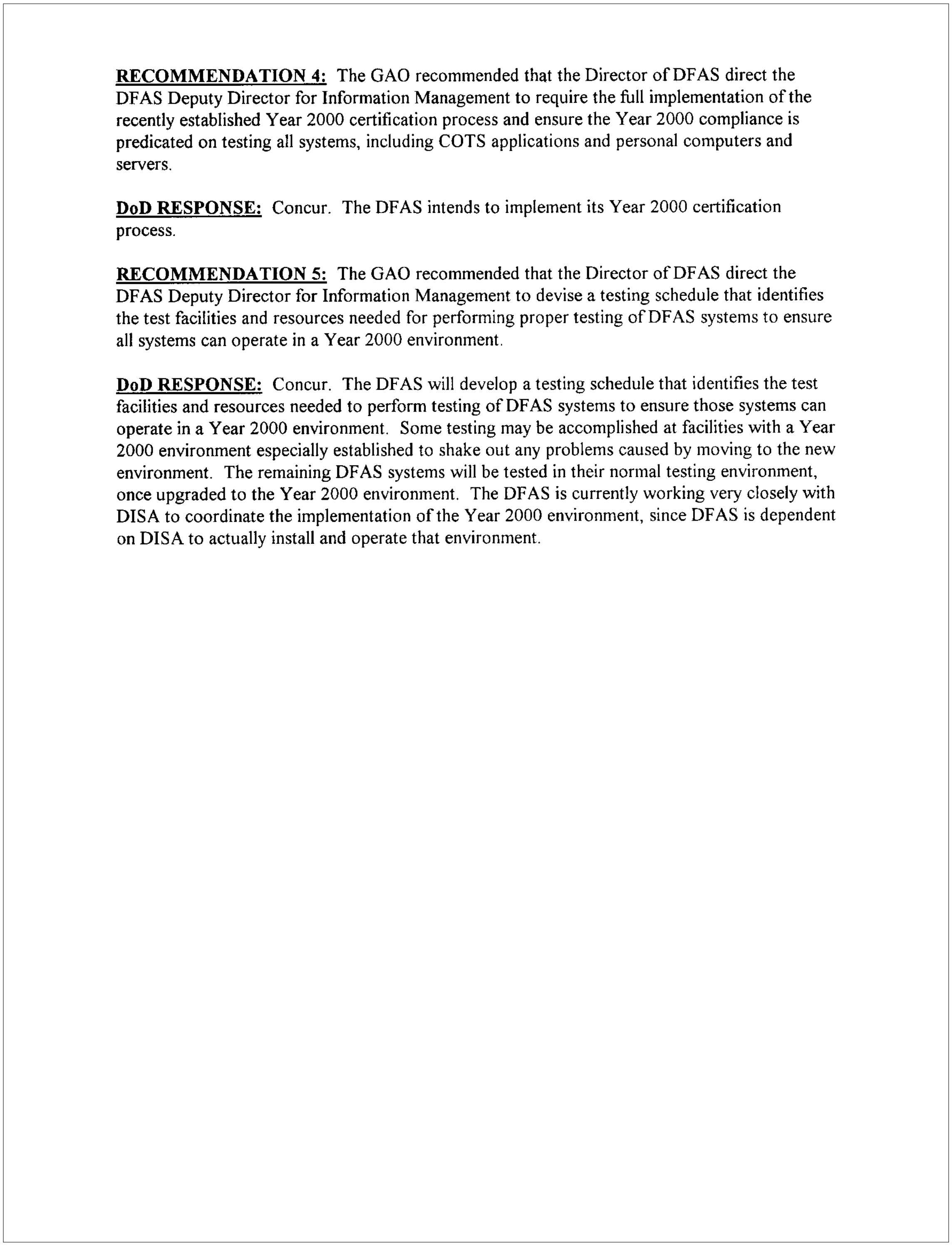
DoD RESPONSE: Concur. The DFAS will update its Year 2000 Executive Plan to incorporate the items listed in the draft report.

RECOMMENDATION 2: The GAO recommended that the Director of DFAS direct the DFAS Deputy Director of Information Management to ensure that DFAS' Corporate Contingency Plan addresses the Year 2000 crisis and provides guidance for ensuring continuity of operations. The guidance should require DFAS managers to perform risk assessments and prepare contingency plans for all critical systems impacted by the Year 2000 that provide data to critical systems. Specifically, risk assessments and contingency plans should be required for all critical systems, including the identifications of alternatives in the event that: (1) replacement systems are not available; (2) systems to be renovated are not completed; and (3) systems fail to operate as intended prior to Year 2000 impact.

DoD RESPONSE: Concur. The DFAS Corporate Contingency Plan, DFAS 3020.26R, is being updated to require a risk assessment and business impact analysis of all mission critical systems and critical direct support systems in regard to the Year 2000 crisis. Included in this update, will be a requirement to test critical systems for Year 2000 compliance and identify contingency strategies for dealing with noncompliant situations.

RECOMMENDATION 3: The GAO recommended that the Director of DFAS direct the DFAS Director for Information Management to require the timely identification of all internal and external systems interfaces and the completion of signed, written interface agreements that describe the method of data exchange between interfacing systems, the entity responsible for performing the system interface modification, and milestones identifying when the modifications is to be completed.

DoD RESPONSE: Concur. The DFAS Program/System Managers have been directed to establish written interface agreements with their interfacing partners by September 30, 1997.



RECOMMENDATION 4: The GAO recommended that the Director of DFAS direct the DFAS Deputy Director for Information Management to require the full implementation of the recently established Year 2000 certification process and ensure the Year 2000 compliance is predicated on testing all systems, including COTS applications and personal computers and servers.

DoD RESPONSE: Concur. The DFAS intends to implement its Year 2000 certification process.

RECOMMENDATION 5: The GAO recommended that the Director of DFAS direct the DFAS Deputy Director for Information Management to devise a testing schedule that identifies the test facilities and resources needed for performing proper testing of DFAS systems to ensure all systems can operate in a Year 2000 environment.

DoD RESPONSE: Concur. The DFAS will develop a testing schedule that identifies the test facilities and resources needed to perform testing of DFAS systems to ensure those systems can operate in a Year 2000 environment. Some testing may be accomplished at facilities with a Year 2000 environment especially established to shake out any problems caused by moving to the new environment. The remaining DFAS systems will be tested in their normal testing environment, once upgraded to the Year 2000 environment. The DFAS is currently working very closely with DISA to coordinate the implementation of the Year 2000 environment, since DFAS is dependent on DISA to actually install and operate that environment.

Major Contributors to This Report

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

Ronald B. Bageant, Assistant Director
Brian C. Spencer, Technical Assistant Director
Brenda A. James, Senior Information Systems Analyst
Cristina T. Chaplain, Communications Analyst

Denver Regional Office

John A. Spence, Information Systems Analyst

Ordering Information

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

Orders by mail:

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

or visit:

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

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

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

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

info@www.gao.gov

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

http://www.gao.gov

PRINTED ON ♻ RECYCLED PAPER