

Audit



Report

YEAR 2000 APPLICATION TESTING AT THE
DEFENSE FINANCE AND ACCOUNTING SERVICE

Report Number 99-231

August 10, 1999

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932 or visit the Inspector General, DoD, Home Page at: www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ADS	Automated Disbursing System
AFSF	Air Force Stock Fund Accounting and Reporting System
CDB	Central Database Accounting System
DCPS	Defense Civilian Pay System
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DJMS-AC	Defense Joint Military Pay System-Active Component
DJMS-RC	Defense Joint Military Pay System-Reserve Component
DLA	Defense Logistics Agency
DRAS-APS	Defense Retiree and Annuitant Pay System-Annuitant Subsystem
DRAS-RCP	Defense Retiree and Annuitant Pay System-Retiree and Casualty Subsystem
DTRS	Defense Transportation Pay System
HQARS	Headquarters Accounting and Reporting System
IAPS	Integrated Accounts Payable System
MCTFS	Marine Corps Total Force System
MOCAS	Mechanization of Contract Administration Services
OASD(C ³ I)	Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
PBAS-FD	Program and Budget Accounting System-Funds Distribution
SIFS	Standard Industrial Fund System
SMAS	Standard Materiel Accounting System
SOMARDS	Standard Operations and Maintenance, Army Research and Development System
SRD-1	Standard Finance System-Redesign, Subsystem 1
STANFINS	Standard Finance System
STARFIARS	Standard Army Financial Inventory Accounting and Reporting System
STARFIARS-MOD	Standard Army Financial Inventory Accounting and Reporting System-Modification
Y2K	Year 2000



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

August 10, 1999

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY

SUBJECT: Audit Report on Year 2000 Application Testing at the Defense Finance and
Accounting Service (Report No. 99-231)

We are providing this report for information and use. We considered management comments on a draft of this report when preparing the final report.

The Defense Finance and Accounting Service comments conformed to the requirements of DoD Directive 7650.3; therefore, additional comments are not required.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Kimberley A. Caprio at (703) 604-9139 (DSN 664-9139) (kcaprio@dodig.osd.mil), or Mr. Michael Perkins at (703) 604-9152 (DSN 664-9152) (mperkins@dodig.osd.mil). See Appendix E for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-231

(Project No. 8FG-6020.01)

August 10, 1999

Year 2000 Application Testing at the Defense Finance and Accounting Service

Executive Summary

Introduction. This is one in a series of reports that the Inspector General, DoD, is issuing in an informal partnership with the DoD Chief Information Officer to monitor DoD efforts to address the Year 2000 computing challenge. For a listing of audit projects addressing the issue, see the Year 2000 website on the IGnet at <http://www.ignet.gov>.

The Defense Finance and Accounting Service (DFAS) uses a monthly status report to track the progress made by its systems toward Year 2000 conversion. The monthly report categorizes systems to be changed, replaced, or terminated; systems in development; and systems that are Year 2000 compliant. Of the 194 systems that were being tracked for Year 2000 progress in January 1999, DFAS considered 65 mission-critical. Of those systems, 42 are active, meaning that they are not currently in development and are not scheduled for replacement or termination before December 31, 1999. Of the 42 active mission-critical systems, 40 reside on domains owned and maintained by the Defense Information Systems Agency.

Objectives. The overall audit objective was to determine the effectiveness of DFAS initiatives to address the Year 2000 computer problem. For this report, we reviewed actions taken to validate the Year 2000 compliance of computer applications for eight active mission-critical systems. These systems, which were selected for their high visibility, are in the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Year 2000 Office and the DFAS Year 2000 Project Office. In addition, we performed a limited review of the remaining 34 mission-critical systems. We also reviewed Defense Logistics Agency efforts to validate the Year 2000 compliance of a Defense Logistics Agency-owned system the Mechanization of Contract Administration Services system, which is used extensively by DFAS.

We did not review the management control program as it relates to the overall audit objective because DFAS and DoD identified Year 2000 conversion problems as an uncorrected material weakness in the FY 1998 Annual Statements of Assurance.

Results. The eight DFAS mission-critical systems met DFAS requirements for application testing during the validation phase of the Year 2000 conversion process. System managers planned, executed, and coordinated system testing to ensure that the systems processed and exchanged date and date-related information accurately in a Year 2000 environment. However, DFAS system managers had insufficient information on the status of domains from

the Defense Information Systems Agency on Year 2000 compliance for 30 out of 40 mission-critical systems. Also, DFAS did not establish written test agreements with the Defense Information Systems Agency for mainframe domains that house 15 systems. As a result, DFAS may certify that systems have tested successfully in Year 2000 environment on a Year 2000-compliant domains (Level 3), although the domains may not be compliant.

The Defense Logistics Agency tested the Mechanization of Contract Administration Services system, used extensively by DFAS for Year 2000 compliance. Test documentation provided evidence of appropriate testing of the system in conformance with the "DoD Year 2000 Management Plan."

Summary of Recommendations. We recommend that the Director, DFAS, require system managers to ascertain from the Inventory/Asset and Configuration Management System the Year 2000 compliance status of each hardware and software product in individual test domains before determining the Level 3 compliance of any DFAS systems that reside on domains owned and maintained by the Defense Information Systems Agency.

Management Comments on the Recommendations. The Director, Information and Technology, DFAS, partially concurred with the recommendation. He stated that DFAS and the Defense Information Systems Agency would jointly review, at the corporate level, the Year 2000 compliance status of each test domain during Level 3 certification testing, to ensure compliance of the domains. However, DFAS does not intend to use the Inventory/Asset and Configuration Management System to ascertain the compliance status of the domains. See the Finding section for a complete discussion of the management comments and the Management Comments section for the text of the comments.

Audit Response. We consider a joint corporate review of test domain compliance to be a responsive corrective action. However, we do not believe that DFAS and the Defense Information Systems Agency will be able to ascertain and document the compliance of hardware and software products on test domains without the Inventory/Asset and Configuration Management System. The Inventory/Asset and Configuration Management System is the only tool available to determine what the Defense Information Systems Agency considers to be the official compliance status of its test domains, and must be used to verify that DFAS systems are being certified on compliant domains. The DFAS should use of the Inventory/Asset and Configuration Management System to conduct and document that review. Because of time constraints, we are not requesting additional comments on the final report. Instead, during future audits, to ensure that DFAS has met the intent of the recommendation, we will review the documentation that DFAS uses to ascertain the compliance status of the Defense Information Systems Agency test domains before granting Level 3 certification to DFAS systems.

Background

Information technology systems have typically used two digits to represent the year, such as "98" representing 1998, to conserve electronic data storage and reduce operating costs. With the two-digit format, however, the year 2000 is indistinguishable from 1900. As a result of the ambiguity, computers, associated systems, and application programs that use dates to calculate, compare, and sort could generate incorrect results when working with years after 1999.

The Deputy Secretary of Defense issued the memorandum, "Year 2000 (Y2K) Verification of National Security Capabilities," on August 24, 1998. The memorandum stated that the Chiefs of Staff of the Military Departments and the Directors of Defense agencies must certify that they have tested their information technology and national security systems in accordance with the "DoD Year 2000 Management Plan." In addition, the Deputy Secretary directed the Principal Staff Assistants of the Office of the Secretary of Defense to verify that all functions under their purview will continue to be unaffected by Year 2000 problems. For the finance and accounting functions, the Under Secretary of Defense (Comptroller) is the Principal Staff Assistant.

DoD Year 2000 Management Plan. The "DoD Year 2000 Management Plan," version 2.0, December 1998 (the Plan), provides guidance to ensure the continuance of DoD operations through January 2000 and beyond. The guidance in the Plan is based on the Government-wide five-phase management process for Y2K conversion. Specifically, the Plan includes guidance for the Year 2000 replacement, repair, testing, and certification of mission-critical systems. The Plan provides details for completing the three approaches necessary for Year 2000 conversion: individual testing and certification, functional end-to-end testing, and joint operational evaluations. In addition, the Plan emphasizes that DoD efforts will shift from system certification to configuration management (ensuring that modifications do not invalidate previous testing) and contingency planning (ensuring that Y2K-related disruptions are identified and minimized).

Defense Finance and Accounting Service Mission and Functions. The Defense Finance and Accounting Service (DFAS) is responsible for DoD finance and accounting functions and the operability of information systems that perform these functions. Each year, DFAS pays over 3 million military and civilian personnel, 2 million retirees and annuitants, and 23 million invoices to contractors and vendors. On a monthly basis, DFAS processes over 9.8 million payments to DoD personnel and over 1 million payments to DoD vendors and contractors; its monthly disbursements exceed \$22 billion. Y2K issues can affect every aspect of the DFAS mission because DFAS relies heavily on computer systems.

Mission-Critical Systems. As of January 1999, DFAS maintains monthly progress reports on the Y2K status of 194 DFAS-owned systems. The monthly reports categorize systems to be changed, replaced, or terminated; those in development; and those that are Y2K compliant. Of the 194 systems being tracked for Y2K progress, DFAS considers 65 mission-critical. Of those

systems, 42 are active, meaning that they are not currently in development and are not scheduled for replacement or termination before December 31, 1999. Of the 42 active mission-critical systems, 40 reside on domains owned and maintained by the Defense Information Systems Agency (DISA).

Mainframe and Mid-Tier Computers. DFAS mission-critical systems generally reside on either mainframe or mid-tier computers.

- Mainframe computers are considered the largest and most powerful category of general-purpose computers. Mainframes are typically housed in a specialized environment that meets specific requirements for temperature, humidity, and electrical power. Mainframes can process several applications at one time and can simultaneously support hundreds of user terminals. DISA owns most mainframe computers and operates them at facilities called Megacenters.
- Mid-tier computers are often called mini-computers and are less powerful than mainframes. Mid-tier computers have many of the operational characteristics and capabilities of mainframe computers, but do not require a specialized environment and are commonly operated in a business office setting.

For purposes of this report, we focused on application testing of mission-critical systems. We included both mainframe and mid-tier mission-critical systems in our review. Inspector General, DoD, Report No. 99-227, "Year 2000 Posture of Mid-Tier Computers Used By the Defense Finance and Accounting Office," issued July 29, 1999, evaluated the Y2K compliance of DFAS systems that reside on mid-tier computers.

Objectives

The overall audit objective was to determine the effectiveness of DFAS initiatives to address the Y2K computer problem. Specifically, in this phase of the audit, we reviewed actions taken to validate the Y2K compliance of applications for eight DFAS mission-critical systems. We selected these eight systems because they were identified by the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (OASD[C³I]) Y2K Office and DFAS officials as highly visible and integral to DoD payments and disbursements (i.e., the payment of civilian and military personnel, retirees, vendors, and contractors). In addition, we performed a limited review of the remaining 34 mission-critical systems that included primarily financial management and accounting systems. We also reviewed the Defense Logistics Agency (DLA) efforts to validate the Y2K compliance of the Mechanization of Contract Administration Services (MOCAS), a DLA owned system used extensively by DFAS.

This is the fourth report on the effectiveness of DFAS Y2K initiatives. The first report covered the DFAS Cleveland Center's performance of system assessments, and the existence and adequacy of interface agreements. The second report evaluated whether DFAS had entered all required data elements into the Defense Integration Support Tools database for each system, and verified that information in that database was consistent with information in DFAS quarterly reports. The third report determined whether DFAS had prepared adequate system-level contingency plans for Y2K, and had reported complete and reliable cost estimates for Y2K systems to the Office of Management and Budget and OASD(C³I).

We did not review the management control program as it relates to the overall audit objective because DFAS and DoD identified Y2K conversion problems as an uncorrected material weakness in the FY 1998 Annual Statements of Assurance. See Appendix A for a discussion of the audit scope and methodology. See Appendix B for a summary of prior audit coverage.

Defense Finance and Accounting Service Year 2000 Application Testing

The eight DFAS mission-critical systems reviewed met the DFAS requirements for application testing during the validation phase of the Y2K conversion process. System managers planned, executed, and coordinated system testing to ensure that the systems processed and exchanged date and date-related information accurately in a Y2K environment. However, for 30 of 40 mission-critical systems, DFAS system managers had insufficient information from DISA on the compliance of domains used for testing. As a result, DFAS may certify that systems have tested successfully in a Y2K environment on a Y2K compliant domains (Level 3), although the domains may not be compliant.

DFAS Policy and Procedures

For a system to be Y2K compliant, multiple parts of the system must be determined to be compliant, including the application, executive software, the hardware, and the domain the system operates on. An application is a computer program designed to perform a certain type of work. An application can manipulate text, numbers, graphics, or a combination. The executive software includes the operating system, which controls the execution of software in the domain and provides services such as resource allocation, scheduling, input/output control, and data management. Hardware is the physical component of a computer system, including the central processing unit and peripherals such as printers, tape silos, and direct access storage devices. A domain is a logical part of a mainframe computer where software is designed to work. DISA owns most mainframe computers and operates them at its Megacenters.

DFAS Regulation 8000.1-R. DFAS Regulation 8000.1-R, "Information Management Policy and Instructional Guidance," version 5.0, October 7, 1997, chapter 3, "Test and Evaluation," establishes policy for the planning, documentation, and execution of testing and evaluation. It outlines the requirements for the four types of testing used by DFAS to determine whether a system functions as intended. A system must successfully pass all four types of testing to move from development into production.

- **Unit Testing:** The first step in testing. Verifies software design and involves testing each unit or development module, and is usually conducted by programmers.
- **Integration Testing:** Tests the application and system for hardware interfaces, data access, external software interfaces, and user requirements.

-
- **Qualification Testing:** Verifies compliance with the system design and performance thresholds and objectives, and is conducted by an independent tester.
 - **Acceptance Testing:** The last step in testing. Validates the acceptability of the system against acceptance criteria in the operational test environment; requires coordination between the system developer and the processing center, usually a Defense Megacenter; and allows both entities to assess the impact of the operating environment on system performance.

The DFAS Y2K Management Plan gives the requirements for the Y2K conversion process for DFAS systems. The Plan requires that the tests outlined in DFAS Regulation 8000.1-R to be conducted to validate Y2K corrections.

DFAS Y2K Management Plan. The “DFAS Year 2000 Management Plan,” Version 1.0, revised October 1998 (the Plan) provides guidance on completing each of the five phases to achieve Y2K compliance. The Plan includes criteria for testing systems and levels for determining Y2K compliance:

- **Level 1** (no longer in use).
- **Level 2:** The system (including interfaces, which are the methods used for exchanging date and date-related information with other systems) has been tested successfully in a Y2K environment. The Director, Information and Technology, DFAS, has stated that Level 2 did not mean “tested successfully in a Y2K environment,” but that the application was compliant and ready to be moved to a Y2K environment.¹
- **Level 3:** The system, including interfaces, has been tested successfully in a Y2K environment on a Y2K-compliant domain.

DFAS Y2K Project Office officials discontinued the use of Level 1 and added Level 3 in October 1998 so that system testing could focus on interfaces and domain testing.

System Testing

DFAS Approach to Y2K Testing. According to the DFAS official responsible for system testing, DFAS is using a business process approach for Y2K testing. DFAS is focusing first on ensuring that all applications are adequately tested.

¹To distinguish between “Y2K environment” and “domain,” we used the definition provided by DFAS testing personnel for the Y2K testing environment (“rolling the system’s dates forward to simulate Y2K conditions”). A domain was defined as “a logical part of a mainframe computer where software is designed to work.” Because “environment” and “domain” are often used interchangeably, we made a distinction between the two terms. We used “Y2K environment” as related to testing conditions or the testing environment, and “domain” for the mainframe or mid-tier computer on which the application resides.

Following completion of the application testing, DFAS plans to perform detailed end-to-end testing. The end-to-end testing will encompass the major pay systems (including civilian, military, vendor, contractor pay systems, and disbursing systems), and supporting systems, as well as interfaces with other organizations that process those pay transactions. For example, the end-to-end test for civilian pay includes a test of transactions initiated at the payroll office, through the DFAS system and the Federal Reserve, to the Department of the Treasury.

For this audit, we selected the following eight active mission-critical systems for a detailed review of the testing of their applications:

- Automated Disbursing System (ADS)
- Defense Civilian Pay System (DCPS)
- Defense Joint Military Pay System-Active Component (DJMS-AC)
- Defense Joint Military Pay System-Reserve Component (DJMS-RC)
- Defense Retiree and Annuitant Pay System-Annuitant Subsystem (DRAS-APS)
- Defense Retiree and Annuitant Pay System-Retiree and Casualty Subsystem (DRAS-RCP)
- Integrated Accounts Payable System (IAPS)
- Marine Corps Total Force System (MCTFS)

We selected these 8 of 42 mission-critical systems because of their high visibility in the OASD(C³I) Y2K Office and the DFAS Y2K Project Office. We reviewed the test plans and results for each system to determine whether personnel had tested the applications in accordance with DFAS testing and Y2K guidance.

Adequacy of DFAS Application Testing. The DFAS Y2K Project Office provided guidance to system managers, monitored system progress toward Y2K validation, and held Y2K summits to discuss testing issues and review selected test plans. Each system planned and conducted appropriate application testing to ensure it that would function correctly in a Y2K environment. As of February 12, 1999, all eight systems had successfully completed DFAS Level 2 Y2K system testing.

Test Plans. Personnel in each system office developed a Y2K test plan. The test plans outlined the process used to identify the timeline of the tests; test procedures (including dates and date calculations to test for); expected results; and other matters of concern. Testing personnel conducted unit testing, integration testing, qualification testing, and acceptance testing to ensure that the systems would function in a Y2K environment. The tests included normal processing in 1999 and 2000, retroactive adjustments from 2000 to 1999, leap year calculations, Julian dates and date calculations, and future date calculations. Testing also included mid-month, end-of-month, and pay period processing at various points in 1999, 2000, and 2001. In addition, the test

plans called for regression testing after future versions of the system were released. In regression testing, the Y2K tests are reapplied to ensure that the new version has not changed the Y2K-compliant code.

Test Execution. The independent Y2K testing was done by DFAS system personnel who were not responsible for making changes to the systems they tested. Test results demonstrated the successful outcome of all the tests outlined above and validated that the systems were Y2K compliant. For example, multiple tests were conducted on DCPS to ensure that it will perform accurately under Y2K conditions. Test results indicated that DCPS is Y2K compliant.

Coordination with Interface Partners and DISA

Successful data exchanges are essential to DFAS operations. DFAS systems interface internally with other DFAS systems and externally with systems belonging to interface partners in the Military Departments, the DoD Components, and various Federal agencies. Data exchanges are critical in the Y2K effort because they can introduce or transmit errors from one organization to another. Coordination with interface partners during testing is important to ensure that information is transmitted accurately under Y2K conditions.

In addition to the proper planning and execution of application testing, each of the eight systems coordinated with interface partners and with DISA personnel to ensure that data would be transmitted accurately in a Y2K environment, and that the systems would run on Y2K-compliant domains.

Interface Partners. DFAS system managers for the eight systems coordinated and conducted live interface testing with interface partners whenever possible. Live interface testing involves sending Y2K test files between an interface partner and the system to ensure that the data are transmitted accurately. In some cases, live testing was not possible because interface partners had not finished renovating their systems for Y2K compliance. In those cases, system managers conducted interface tests using test files that simulated date information from the interface partner. Live interface testing is preferable to simulated testing because live testing allows the systems to actively transfer information to verifying the method of transfer.

For example, live and simulated interface testing was conducted for DRAS-RCP. DRAS-RCP conducted live interface testing with the Defense Debt Management System, for which Y2K renovations were completed. DRAS-RCP personnel also conducted simulated interface testing with the Personnel Data System, for which Y2K renovations were not completed. For the interface test, DRAS-RCP testing personnel created a personnel data system file with two-digit years under Y2K conditions, and during the processing, the system converted the file to four-digit years. Test results showed that both interfaces were accurately processed through the system.

Defense Information Systems Agency. We evaluated the coordination between DFAS and DISA for 40 mission-critical systems. DISA owns and maintains domains for 40 of the 42 DFAS active mission-critical systems. The remaining two systems run on domains owned and maintained by DFAS and the Army. To complete Y2K testing, DFAS must coordinate with DISA to ensure that systems can test on Y2K-compliant domains. DFAS assigns personnel to serve as DISA liaisons to ensure that the systems can test and implement compliant systems on Y2K-compliant domains. Without compliant domains, systems cannot be fully validated for Y2K compliance. We performed detailed reviews for the eight mission-critical systems. For the remaining 32 mission-critical systems, we met with system and technical managers to determine the level of coordination with DISA.

Adequacy of Coordination with DISA. We identified two issues regarding the adequacy of coordination between DFAS and DISA. Specifically, DFAS system managers received insufficient information to support verification that DISA domains were Y2K-compliant before DFAS tested applications on the domains. Also, because of unforeseen delays incurred by DISA and other non-DFAS applications using DISA domains, some DFAS systems were delayed in achieving Level 3 Y2K assurance.

Information on Status of Domains. As of February 12, 1999, 8 of the 40 applicable mission-critical systems had not received any information from DISA regarding the domain. Of the 40 systems, 22 received verbal notice that the domain was compliant, and the remaining 10 systems received written notice of domain compliance (for example, an e-mail message from DISA personnel to the DFAS liaison, or a list of compliant vendor-supplied software resident on the domain).

On July 2, 1998, the Deputy Secretary of Defense directed that written agreements be established between DISA and domain users. Further, on August 7, 1998, the Secretary of Defense issued a memorandum stating that funds were not to be obligated for any domain user failing to sign an explicit Y2K test agreement with DISA by October 1, 1998.

Of the 40 DFAS active mission-critical systems residing on DISA domains, 6 are on mid-tier computers. Also, for three systems, testing was conducted on a domain maintained by the Standard Systems Group, Montgomery, Alabama. According to the Secretary of Defense's memorandum, the remaining 31 systems should have Y2K test agreements with DISA. However, only 16 systems had a written agreement. One system had a draft agreement, and one system had a verbal agreement. System personnel at the remaining 13 systems stated that either they did not have a test agreement, or did not know whether they had one. In addition, although some agreements were signed and in place, those agreements did not identify dates when DISA domains must be compliant, and did not establish requirements that DISA provide formal notice to DFAS to validate that the relevant DISA domain was compliant.

DISA did not provide any documentation to show DFAS system personnel that testing was performed and the domain was Y2K compliant for the 30 systems. Without this documentation, DFAS system managers had to rely on DISA

verbal notification or good faith in DISA concerning the domain's Y2K compliance. One of the eight systems continued with its testing although it did not receive any information (verbal or written) from DISA regarding the Y2K compliance of its domain. The system has been certified as Level 3 compliant, although no information is available on the Y2K status of its domain. Therefore, the Level 3 certification may not be valid.

Delays in Domain Compliance. DFAS systems have been prevented from completing the Y2K conversion process because of delays by DISA in providing Y2K-compliant domains. Although the systems have completed DFAS Level 2 testing, in many cases, they have been unable to complete DFAS Level 3 testing and implementation because DISA has not completed work to ensure Y2K-compliant domains. As of February 12, 1999, 13 of the 40 applicable mission-critical systems were waiting for a Y2K-compliant domain to complete the Y2K conversion process.

For example, DFAS has completed Y2K compliance testing on the application for the DJMS-AC. DJMS-AC uses the DISA-owned domain at the Defense Megacenters Chambersburg, Chambersburg, Pennsylvania. DISA has experienced delays in achieving Y2K compliance for the domain at the Defense Megacenters Chambersburg because the domain was originally scheduled to be closed before December 31, 1999, but DISA and Navy officials later agreed to keep it open until after January 1, 2000. DISA officials informed us that the executive software for the domain was scheduled to be compliant by May 31, 1999, and the last of its applications was to complete testing by November 30, 1999. However, in February 1999, officials from the Inspector General, DoD; DISA; and the OASD(C³I) Y2K Office discussed the late 1999 date. After the meeting, DISA revised the date that the domain will be compliant to September 3, 1999.

We are concerned that not being able to test DJMS-AC until after September 3, 1999, puts significant pressure on DFAS, DISA, and other related parties. They will need to conduct test to ensure that they correct all Y2K problems with DJMS-AC, its related executive software and applications, DISA domain and executive software, and any other applications on the domain. Although DFAS intends to conduct end-to-end testing on DJMS-AC, it must delay the testing until the domain at the Defense Megacenters Chambersburg is validated as Y2K-compliant. The short time frame puts pressure on DISA to accommodate the 71 applications on the domain, if they all wish to conduct end-to-end testing. We believe there is an increased risk of production domain and application failure at the Defense Megacenters Chambersburg. The risk is caused by the lack of time remaining to conduct end-to-end testing and correct any unexpected problems that may arise after the last application on the production domain is validated.

Recent Efforts to Ensure Coordination. DFAS systems are critical to ensuring that military and civilian personnel, reservists, retirees, annuitants, vendors, and contractors receive timely pay before, during, and after 2000. In addition, DFAS systems provide support for the DoD financial statements. Therefore, these systems, including the DISA domains they reside on, must be tested adequately for Y2K compliance. Officials in the DFAS Y2K Project office are aware of the problems with DISA domains, and are monitoring DISA

efforts to provide Y2K-compliant domains for testing and production. During a March 5, 1999, meeting between the Assistant Inspector General for Auditing, the Principal Deputy for Y2K, OASD (C³I), and the Commander, DISA Western Hemisphere, we brought the issue of DISA domains to their attention and were assured that DISA is working to resolve its Y2K issues quickly. In Inspector General, DoD, Report No. 99-182, "DISA Management of Mainframes," issued on June 9, 1999, we reported on the progress being made toward domain compliance at the Defense Megacenters. We commend the Principal Deputy for Y2K, OASD(C³I), for acknowledging that DISA needs to work more closely with domain users and ensure that the users have compliant domains as soon as possible for testing purposes, as well as accurate information regarding Y2K compliance of DISA domains. Before determining Level 3 compliance for any DFAS systems that reside on the domains, DFAS system managers should ascertain from the Inventory/Asset and Configuration Management System the Y2K compliance status of each hardware and software product in individual test domains.

Update on Y2K Compliance at the Defense Megacenter Chambersburg. In comments on this report, the Director, Information and Technology, DFAS, stated that because DJMS-AC runs at multiple Defense Megacenters, the delay in achieving a Y2K-compliant domain at the Defense Megacenter Chambersburg was an implementation issue, not a certification issue. He stated that certification for DJMS-AC was completed at the Defense Megacenter Denver, Denver, Colorado, in February 1999. He also stated that the application was implemented at the Defense Megacenter Chambersburg in April 1999, when the Y2K-compliant hardware, executive software, and third-party software needed specifically for DJMS-AC were available on the production domain.

When an application runs on more than one domain, it is important to ensure that all of the domains are certified before implementation. Although the Defense Megacenter Denver was certified in February 1999, the Defense Megacenter Chambersburg was not. According to DISA, some executive software issues would not be resolved until May 31, 1999, and other applications would not be compliant until September 3, 1999. Unless all executive software and all applications that run on a domain are certified, there is an increased risk that the DFAS application will not be able to correctly process dates and date-related information under Y2K conditions.

Implementation of Mission-Critical Systems

The Office of Management and Budget set a deadline of March 31, 1999, for the implementation of Y2K-compliant systems. According to the The Plan, the implementation phase ends when all interfaces are ready to handle noncompliant data; when risk management and contingency strategies have been updated and distributed; and when the "renovated, validated, and certified" system has been successfully deployed in the operational environment (domain). DFAS reported that it had implemented 29 of 42 active mission-critical systems by the deadline. The following systems did not meet the deadline:

-
- Automated Disbursing System (ADS)
 - Air Force Stock Fund Accounting and Reporting System (AFSF)
 - Central Database Accounting System (CDB)
 - Defense Retiree and Annuitant Pay System-Retiree and Casualty Subsystem (DRAS-RCP)
 - Defense Transportation Pay System (DTRS)
 - Headquarters Accounting and Reporting System (HQARS)
 - Program and Budget Accounting System-Funds Distribution (PBAS-FD)
 - Standard Industrial Fund System (SIFS)
 - Standard Materiel Accounting System (SMAS)
 - Standard Operations and Maintenance, Army Research and Development System (SOMARDS)
 - Standard Finance System-Redesign, Subsystem 1 (SRD-1)
 - Standard Finance System (STANFINS)
 - Standard Army Financial Inventory Accounting and Reporting System-Modification (STARFIARS-MOD)

System managers had scheduled 7 of the 13 systems for implementation by April 30, 1999. Four systems had completed all requirements for implementation before March 31, 1999. However, because one monthly accounting cycle is needed to integrate a module into the operational environment, system managers were unable to fully integrate the compliant modules into the production domains during the March cycle, and were required to wait until the April cycle. DFAS officials stated that ADS, AFSF, CDB, and DRAS-RCP had validated and certified their systems in March, but system managers planned to integrate the Y2K-compliant modules during the April accounting cycle. They anticipated that those systems would be implemented by April 16, 1999. In addition, DFAS officials expected that DTRS, HQARS, and PBAS-FD would be implemented by April 30, 1999. They stated that the remaining six systems were scheduled to be implemented by September 30, 1999. SIFS, SOMARDS, SRD-1, and STANFINS were scheduled for implementation by May 31, 1999; SMAS should have been implemented by June 30, 1999; and STARFIARS-MOD should have been implemented by September 30, 1999. Until a system has been implemented, it should be considered high-risk.

DFAS Update on the Implementation Status of Mission-Critical Systems.

The Director, Information and Technology, DFAS, stated that 10 of the mission-critical systems were not compliant. He also stated that SRD-1, STANFINS, and STARFIARS-MOD were to be tested for certification and were scheduled to be implemented in July 1999.

Update on Implementation Status of Mission-Critical Systems. The DFAS Y2K Monthly Status Report for the month ending June 30, 1999, shows that DFAS certified and implemented 10 of the 13 systems. The DFAS presentation on Y2K status to the Secretary of Defense on July 21, 1999, showed the following dates for implementation of the remaining three systems:

- August 13, 1999, for SRD-1;
- August 15, 1999, for STARFIARS-MOD; and
- September 15, 1999, for STANFINS.

Although the renovation of STARFIARS was completed in March 1999, implementation did not begin until July 15, 1999, and is scheduled to be completed on September 15, 1999. This is 1 month after the implementation of STARFIARS-MOD; however, STARFIARS is intended to be the Y2K backup for STARFIARS-MOD. Therefore, there is still a high risk that the three remaining mission-critical systems will not complete their Y2K conversions and will not be able to participate in end-to-end testing of critical business processes for DFAS.

Mechanization of Contract Administration Services System

We included the Mechanization of Contract Administration Services (MOCAS) in our review because the MOCAS system provides important financial data to DFAS. MOCAS is a DLA-owned system that is used extensively by DFAS.

DFAS uses MOCAS data to pay more than 1.2 million contractor invoices valued at more than \$69 billion annually. If Y2K problems cause a MOCAS system failure, DFAS could be unable to pay contractor invoices.

MOCAS has several subsystems, some of which run on mainframe domains and some on mid-tier domains. For this audit, we limited our review to the adequacy of Y2K application testing of the mainframe subsystems. The Inspector General, DoD, Report No. 99-227, "Year 2000 Posture on Mid-Tier Computers Used By the Defense Finance and Accounting Office" issued July 29, 1999, addresses the adequacy of MOCAS applications run on mid-tier domains.

MOCAS Y2K Compliance. DFAS relies on DLA to maintain MOCAS and ensure that the system is Y2K-compliant. We met with DFAS and DLA personnel regarding MOCAS Y2K compliance and reviewed pertinent test documentation. The MOCAS system manager planned, executed, and coordinated system testing to ensure that the MOCAS system processed and exchanged date and date-related information accurately in a Y2K environment. In addition, DLA officials stated that the MOCAS system will participate in end-to-end testing (a functional test under Y2K conditions that includes live data exchanges with all interface partners), which should further validate the

system's Y2K compliance. Based on our limited review, we believe that MOCAS personnel have appropriately tested the subsystem that resides on mainframe domains for Y2K conversion to meet the requirements of the The Plan.

Conclusion

For each of the eight DFAS mission-critical systems, personnel ensured that the applications met the DFAS requirements for the validation phase of the Y2K conversion process. Testing personnel developed test plans in accordance with guidance and conducted appropriate application testing to ensure that the systems were Y2K-compliant. They coordinated with interface partners and conducted interface tests to ensure that date and date-related information were transmitted accurately under Y2K conditions. DLA personnel also conducted appropriate Y2K testing of MOCAS. However, DFAS system managers received insufficient information from DISA about the compliance of domains being used for testing. In addition, for the mainframe domains that housed 15 of 31 systems, DFAS and DISA neither established written test agreements nor effectively exchanged information by other means. As a result, DFAS may certify that systems have been tested successfully in a Y2K environment on a Y2K-compliant domain, although the systems' domains may not yet be compliant.

Recommendation, Management Comments, and Audit Response

We recommend that the Director, Defense Finance and Accounting Service, require system managers to ascertain, from the Inventory/Asset and Configuration Management System, the Year 2000 compliance status of each hardware and software product in individual test domains prior to determining Level 3 compliance for any Defense Finance and Accounting Service systems that reside on the domain.

Management Comments. The Director, Information and Technology, DFAS, partially concurred, stating that DFAS and DISA will, at a corporate level, jointly review the compliance status of each test domain at the time of Level 3 certification testing for DFAS systems. The Director also stated that although the Inventory/Asset and Configuration Management System may be used to verify the compliance of some products, DFAS will not require individual system managers to use that system.

Audit Response. We consider a joint corporate review of test domain compliance to be a responsive corrective action. However, we do not believe that DFAS and DISA will be able to ascertain and document the compliance status of each hardware and software product that resides on DISA test domains without using the Inventory/Asset and Configuration Management System. The

Inventory/Asset and Configuration Management System is the only tool available to determine what DISA considers to be the official compliance status of its test domains, and must be used to verify that DFAS systems are being certified on compliant domains. We also note that regardless of Y2K issues, system managers need to know the configuration management status of the executive software on their test domains; the Inventory/Asset and Configuration Management System provides that information.

Because of time constraints, we will not request additional comments on the final report. Instead, during future audits, to ensure that DFAS has met the intent of the recommendation, we will review the documentation that DFAS uses to ascertain the compliance status of the DISA test domains before granting Level 3 certification to DFAS systems.

Appendix A. Audit Process

This report is one in a series being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the Y2K computing challenge. For a list of audit projects addressing this issue, see the Y2K website on the IGnet at <http://www.ignet.gov>.

Scope and Methodology

This report is a continuation of a prior audit. In Inspector General, DoD, Report No. 99-049, "Year 2000 Contingency Planning and Cost Reporting at the Defense Finance and Accounting Service," December 10, 1998, we reviewed DFAS progress in resolving Y2K computing issues. This report is based on audit fieldwork performed from October 1998 through February 1999 at DFAS Headquarters, Arlington, Virginia; the Cleveland DFAS Center, Cleveland, Ohio; the DFAS Columbus Center, Columbus, Ohio; the DFAS Denver Center, Denver, Colorado; the DFAS Indianapolis Center, Indianapolis, Indiana; and the DFAS Kansas City Center, Kansas City, Missouri; Systems Engineering Organization, Pensacola, Florida; and Standard Systems Group, Montgomery, Alabama.

We selected systems from the DFAS October 1998 monthly report submitted to the Director, Information and Technology, DFAS. The monthly report showed that DFAS tracked 42 active mission-critical finance and accounting systems (see Appendix C for the list of DFAS mission-critical systems). Of the 42 systems, we selected 8 systems for a detailed review. We selected the 8 systems, which are used for payroll, vendor pay, and disbursing, because the OASD(C³I) Y2K Office and DFAS officials considered them highly visible. We also reviewed MOCAS, a DLA system, because it provides important financial data to DFAS. See Appendix D for background information on the systems selected for review.

We interviewed personnel at the OASD(C³I) Y2K Office and the DFAS Y2K project office. We interviewed DFAS system managers in the functional and technical areas at DFAS Headquarters and the DFAS Cleveland, Columbus, Denver, Indianapolis, and Kansas City Centers. We also interviewed DLA personnel at the DFAS Columbus Center. In addition, we interviewed technical managers at the Pensacola and Montgomery system design activities. We also reviewed test plans and test results to determine compliance with the DoD and DFAS Y2K Management Plans. In addition, we contacted the managers of all 42 mission-critical systems, and determined their awareness of DISA domain Y2K compliance.

DoD-Wide Corporate-Level Goals. In response to the Government Performance and Results Act, DoD has established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting the objectives. This report pertains to achievement of the following objective and goal.

Objective: Fundamentally reengineer the Department and achieve a 21st century infrastructure. **Goal:** Reduce costs while maintaining required military capabilities across all DoD mission areas. **(DoD-6)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objective and goal.

Financial Management Functional Area. Objective: Reengineer DoD business practices. **Goal:** Modify existing systems and monitor new systems to ensure Y2K compliance. **(FM-4.3)**

General Accounting Office High-Risk Area. In its identification of risk areas, the General Accounting Office has specifically designated resolution of the Y2K problem as high-risk. This report provides coverage of this problem and of the overall Information Management and Technology high-risk area.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Use of Technical Assistance. Technical experts in our Audit Followup and Technical Support Directorate provided information on ongoing evaluations of DISA domains and software development and maintenance issues.

Audit Type, Dates, and Standards. We performed this financial-related audit by reviewing test plans dated between October 1997 and November 1998, and documentation of test results dated between September 1998 and February 1999, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD.

Contacts During the Audit. We visited or contracted individuals and organizations within DoD. Further details are available on request.

Management Control Program. We did not review the management control program as it relates to the overall objective. DFAS and DoD identified Y2K as an uncorrected material weakness in their Annual Statements of Assurance for FY 1998.

Appendix B. Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to DFAS Y2K issues. General Accounting Office reports can be accessed on the Internet at <http://www.gao.gov>. Inspector General, DoD reports can be accessed on the Internet at <http://www.dodig.osd.mil>.

General Accounting Office

GAO Report No. AIMD-97-117 (OSD Case No. 1392), "Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem," August 11, 1997.

Inspector General, DoD

Inspector General, DoD, Report No. 98-112, "Year 2000 Reporting for Defense Finance and Accounting Service Cleveland Center Systems," April 17, 1998.

Inspector General, DoD, Report No. 98-111, "Year 2000 Initiatives at the Defense Finance and Accounting Service Cleveland Center," April 16, 1998.

Inspector General, DoD, Report No. 99-049, "Year 2000 Contingency Planning and Cost Reporting at the Defense Finance and Accounting Service," December 10, 1998.

Inspector General, DoD, Report No. 99-182, "DISA Management of Mainframes," June 9, 1999.

Inspector General, DoD, Report No. 99-227, "Year 2000 Posture of Mid-Tier Computers Used By the Defense Finance and Accounting Office," July 29, 1999.

Appendix C. Defense Finance and Accounting Service Active* Mission-Critical Systems

The following systems are principally owned by DFAS and were defined as mission-critical in the DFAS Y2K monthly status report for January 1999. Systems that are in development or scheduled for replacement or termination are not listed. We performed in-depth reviews of the 8 systems shown in bold type, and an overall review of the 34 remaining systems.

Automated Disbursing System (ADS)

Air Force Stock Fund Accounting and Reporting System (AFSF)

AVFuels Management Accounting System (AMAS)

Computerized Accounts Payable System (Clipper version) (CAPS-C)

Central Database Accounting System (CDB)

Centralized Expenditure/Reimbursement Processing System (CERPS)

Case Management Control System-Accounting Segment (CMCS)

Command On-line Accounting and Reporting System (COARS)

Central Procurement Accounting System (CPAS)

Defense Business Management System (DBMS)

Defense Civilian Pay System (DCPS)

Defense Debt Management System (DDMS)

Defense Industrial Financial Management System (DIFMS)

Defense Integrated Financial System (DIFS)

Defense Joint Military Pay System-Active Component (DJMS-AC)

Defense Joint Military Pay System-Reserve Component (DJMS-RC)

Defense Retiree and Annuitant Pay System-Annuitant Pay System (DRAS-APS)

Defense Retiree and Annuitant Pay System-Retiree and Casualty Pay System (DRAS-RCP)

Defense Transportation Pay System (DTRS)

Defense Working Capital Accounting System (DWAS)

Financial Reporting System-Accounting (FRS-ACCTG)

General Accounting and Finance System-Base Level (GAFS)

General Funds General Ledger System (GFGL)

Headquarters Accounting and Reporting System (HQARS)

Integrated Accounts Payable System (IAPS)

Integrated Automated Travel System (IATS)

Industrial Fund Accounting System (IFAS)

Integrated Paying and Collecting System (IPC)

Merged Accountability and Fund Reporting System (MAFR)

Marine Corps Total Force System (MCTFS)

Military Traffic Management Command-Financial Management System (MTMC-FMS)

Program and Budget Accounting System-Funds Distribution (PBAS-FD)

Standard Accounting Budgeting and Reporting System (SABRS)

Standard Industrial Fund System (SIFS)

* Active means that the system was not in development and was not scheduled for replacement or termination before December 31, 1999.

Standard Materiel Accounting System (SMAS)
Standard Negotiable Instrument Processing System (SNIPS)
Status of Funds System (SOF)
Standard Operations and Maintenance, Army Research and Development System (SOMARDS)
Standard Finance System Redesign, Subsystem 1 (SRD-1)
Standard Finance System (STANFINS)
Standard Army Financial Inventory Accounting and Reporting System–Modified (STARFIARS-MOD)
Standard Accounting and Reporting System (STARS)

Appendix D. Background Information on Systems Selected for Review

Automated Disbursing System. ADS automates disbursing and accounting functions in several departments at the DFAS Cleveland Center. ADS automates entries into the Financial Reporting System and eliminates the need for manual posting of daily transactions to a cashbook or spreadsheet.

Defense Civilian Pay System. DCPS is the payroll system for civilian employees in DoD. The system maintains pay and leave entitlement records, deductions and withholdings, time and attendance data, and other pertinent employee data. DCPS serves 727,000 DoD employees worldwide and is supported by 3 payroll offices and 2 disbursing centers.

Defense Joint Military Pay System-Active Component. DJMS is the payroll system for all active-duty and Reserve military members of the Army, Navy, Air Force, and the military Academies, and includes two components. DJMS maintains 1,126,000 Army payment accounts, 584,000 Air Force payment accounts, and 655,000 Navy accounts. DJMS-AC handles all Army, Navy, and Air Force active-duty military personnel and military academy cadets and midshipmen.

Defense Joint Military Pay System-Reserve Component. DJMS-RC handles payroll processing for all Army, Navy, and Air Force Reserve personnel.

Defense Retiree and Annuitant Pay System-Annuitant Pay Subsystem. DRAS-APS is the subsystem used to pay military annuitants of the Army, Navy, Air Force, and Marine Corps. DRAS-APS pays an average monthly payroll of \$139 million to 254,000 annuitants. DRAS-APS is supported by 884 users at 150 DoD sites.

Defense Retiree and Annuitant Pay System-Retiree and Casualty Pay Subsystem. DRAS-RCP is the subsystem that pays retirees of the Army, Navy, Air Force, and Marine Corps. The system is responsible for disbursing pay to retired military personnel and former spouses, and pays 1.9 million accounts worldwide, with an average monthly payroll of \$2.5 billion.

Integrated Accounts Payable System. IAPS provides automatic processing for accounts payable transactions to vendors for local purchases. IAPS generates payment vouchers, performs automatic reconciliation, and provides automatic followup for missing documents.

Mechanization of Contract Administration Services. MOCAS is a DLA-owned automated system used to administer and pay supply and service contracts. DFAS uses MOCAS data to pay over 1.2 million contractor invoices valued at more than \$69 billion annually.

Marine Corps Total Force System. MCTFS is an integrated pay and personnel system that supports the active-duty and Reserve Components of the Marine Corps and the personnel management of all retired Marines. MCTFS is the pay system for 174,000 active-duty Marines, 40,000 Selected Reserve Marines, and 57,000 Individual Ready Reserve Marines.

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Deputy Assistant Secretary of Defense (Command, Control, Communications, and Intelligence, Surveillance, Reconnaissance, and Space Systems)
Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer, Policy and Implementation)
Principal Director for Year 2000

Joint Staff

Director, Joint Staff

Department of the Army

Auditor General, Department of the Army
Inspector General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy
Chief Information Officer, Navy
Inspector General, Department of the Navy
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Air Force Audit Agency
Chief Information Officer, Air Force
Inspector General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
 Director for Information and Technology
Director, Defense Information Systems Agency
 Inspector General, Defense Information Systems Agency
 Chief Information Officer, Defense Information Systems Agency
 United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
 Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
 Office of Information and Regulatory Affairs
General Accounting Office
 National Security and International Affairs Division
 Technical Information Center

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Technology Problem
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology,
 Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International
 Relations, Committee on Government Reform
House Subcommittee on Technology, Committee on Science

Defense Finance and Accounting Service Comments



DFAS-HQ/S

DEFENSE FINANCE AND ACCOUNTING SERVICE

1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

JUN 9 1999

MEMORANDUM FOR DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE
OFFICE OF THE INSPECTOR GENERAL
INSPECTOR GENERAL

SUBJECT: Audit Report on Year 2000 Application Testing at the
Defense Finance and Accounting Service
(Project No. 8PG-6020.01)

This memorandum is in response to the Department of Defense (DoD), Inspector General's (IG) draft report after review of the Defense Finance and Accounting Service (DFAS) application testing. Additional comments and clarifications are attached.

Recommendation. We recommend that the Director, Defense Finance and Accounting Service, require system managers to ascertain, from the Inventory/Asset and Configuration Management System, the Year 2000 compliance status of each hardware and software product in individual test domains prior to determining Level 3, compliance for any Defense Finance and Accounting Service systems that reside on that domain.

Response. Partially concur. DFAS and DISA will, at a corporate level, jointly review the Year 2000 compliance status of each test domain at the time of Level 3, certification testing to ensure the domains were compliant. Although the Inventory/Asset and Configuration Management System may be used to verify the status of some products, DFAS will not require individual system managers to use that system.

Any questions regarding this response can be directed to my point of contact, Sharon Brustad, DFAS-HQ/SB, (317) 510-5647.


C. Vance Kauzlarich
Director, Information and Technology

Attachment

Three statements in the report need to be corrected or clarified.

1. This report incorrectly identifies the three DFAS certification levels. Level 1, had nothing to do with "using software to roll the system's dates forward to simulate Y2K conditions." It was established to track systems that had completed Y2K changes, or were developed compliant, but were still working on interface agreements. Level 2, does not mean "tested successfully in a Y2K environment". It means the application was compliant and ready to be moved to a Y2K environment. It should also be noted that all DFAS systems must accomplish DFAS Level 3 certification. The correct definitions for the DFAS Certification Levels are:

Level 1 - (no longer used) The system is considered compliant yet one or more interface agreements have not been completed. The system must have completed all necessary testing and has either been implemented or is in the process of being implemented. All interfaces currently under written agreements must have been implemented according to those agreements.

Level 2 - The system has been tested and found compliant. If the system has interfaces, all interfaces have been tested, either with the partner or through simulation, and found compliant. All interfaces are in the format agreed to by the interfacing partners, or will be modified by a future date that has been mutually agreed upon. Testing was performed on an environment that is not Y2K compliant.

Level 3 - The system has been tested and found compliant. If the system has interfaces, all interfaces have been tested, either with the partner or through simulation, and found compliant. All interfaces are in the format agreed to by the interfacing partners, or will be modified by a future date that has been mutually agreed upon. Testing was performed on an environment that is considered Y2K compliant.

2. This report incorrectly states that DJMS-AC would not be able to test until after September 3, 1999. Because DJMS-AC runs at multiple Megacenters, the delay in achieving a Y2K compliant domain in Chambersburg was an implementation issue not a certification testing issue. Certification for DJMS-AC was completed in February 1999 at DMC Denver. The application was implemented at Chambersburg in April 1999 which was when the Y2K compliant hardware, executive software, and 3rd party COTS

products needed for DJMS-AC were available on the production domain.

3. To clarify the implementation status of the DFAS systems, all but three of the 13 mission critical systems listed in the report have been implemented. The three systems, Standard Finance System (STANFINS), Standard Finance System-Redesign (Subsystem 1) (SRD1), and Standards Army Financial Inventory Accounting and Reporting System - Modification (STARFIARS-MOD), are currently in certification testing and scheduled to be implemented in July 1999. In addition DFAS has renovated the Standards Army Financial Inventory Accounting and Reporting System (STARFIARS) to ensure any site that has not converted to STARFIARS-MOD before October 1, 1999 will be running on a compliant version of software. STARFIARS has completed renovation and is scheduled to complete implementation in July 1999.

Audit Team Members

The Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report.

F. Jay Lane
Kimberely A. Caprio
Michael Perkins
Daniel B. Convis
Laura A. Rainey
William C. Coker
Charlene K. Grondine
Robyn N. Stanley
Susanne B. Allen