Evaluation Report

EVALUATION OF THE DEFENSE MEGACENTERS
YEAR 2000 PROGRAM

Report Number 98-193

August 25, 1998

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 Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932 of visit the Inspector General, DOD, Home Page at: WWW.DODIG.OSD.MIL

Suggestions for Future Evaluations

To suggest ideas for or to request future evaluations, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: APTS Evaluation Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, Virginia 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, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
CDA	Central Design Activity
DISA	Defense Information Systems Agency
DISA WESTHEM	Defense Information Systems Agency Western Hemisphere
DMC	Defense Megacenter
DSA-D	Defense Information Systems Agency Support Activity – Denver
OSD	Office of the Secretary of Defense
SOE	Standard Operating Environment
SSO	System Support Office
Y2K	Year 2000

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

August 25, 1998

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)/ DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Evaluation of the Defense Megacenters Year 2000 Program (Report No. 98-193)

We are providing this report for information and use. Management comments on a draft were considered in preparing the final report.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the evaluation staff. Questions on the evaluation should be directed to Mr. Kenneth Stavenjord, at (703) 604-8952 (DSN 664-8952) (kstavenjord@dodig.osd.mil) or Mr. Dan Convis, at (703) 602-1769 (DSN 332-1769) (dconvis@dodig.osd.mil). See Appendix C for the report distribution. The evaluation team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-193 **August 25, 1998**
(Project No. 8PT-3005)

Evaluation of the Defense Megacenters Year 2000 Program

Executive Summary

Introduction. This is one of a series of reports 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 Year 2000 computing challenge. Our attention focused on the Defense Megacenters because they are primary providers of mainframe computer services to functional users in the Air Force, Army, Navy, Marine Corps, and the Defense agencies. The systems that run on a mainframe computer operate in a logical partition called a "domain."

Evaluation Objectives. The evaluation objective was to determine whether the Defense Information Systems Agency was adequately preparing its information technology systems at its Defense Megacenters to resolve Year 2000 date processing issues. We evaluated Year 2000 readiness of executive software running on mainframe computers at the Defense Information Systems Agency's Defense Megacenters. We also included the Year 2000 readiness of the hardware and facilities used to support the executive software. Our evaluation report is based on our field work that was completed on May 4, 1998. In addition, actions undertaken after May 4 but prior to the issuance of our report were acknowledged.

Evaluation Results. Although much progress has been made in converting the Defense Megacenters Systems to Year 2000 compliance, problems remain in three areas: reporting, testing, and contingency planning.

- Defense Information Systems Agency Year 2000 status reports for executive software were incomplete and could be misinterpreted. The reports showed that the executive software product inventory was 60 percent compliant but did not reveal that the domain compliance was zero percent. As a result, DoD is at risk of classifying mission critical systems on mainframe computers as being Year 2000 compliant when they are not (Finding A).

- The Defense Information Systems Agency did not plan to test the non-Standard Operating environment, computer hardware, and facility equipment for Year 2000 compliance. As a result, mission critical processing may be at risk of date related failures (Finding B).

- Although the Defense Information Systems Agency decided to establish contingency plans and issue initial guidance to the Defense Megacenters, the guidance needs to be expanded. Without comprehensive planning, mission critical systems may not be able to continue operations if Year 2000 failures occur (Finding C).

The results of the evaluation were briefed to the Director, Defense Information Systems Agency on June 26, 1998 and to the Deputy Secretary of Defense on July 22, 1998. In both cases, management directed that corrective actions be initiated immediately.

Summary of Recommendations. We recommend that the Director, Defense Information Systems Agency (DISA) direct the Defense Megacenters and System Support Office to establish written agreements with the Central Design Activities for domain renovations, report complete Year 2000 status including executive software renovations by domain, and report the affected applications by domain. We recommend that DISA report domain Year 2000 compliance status to the Office of the Secretary of Defense. We recommend that the Department of Defense Chief Information Officer direct the Central Design Activities to expedite establishment of written agreements with the Defense Megacenters and Systems Support Office for domain executive software Year 2000 renovation. We recommend that the Department of Defense Chief Information Officer advise the Secretaries of the Military Departments and Defense agencies when domains have a high risk of not becoming Year 2000 ready. We recommend that DISA direct the Defense Megacenters and System Support Office to implement comprehensive Year 2000 testing of non-standard executive software, computer hardware, and facility equipment. We recommend that DISA require the writing of contingency plans by the Defense Megacenters and that these contingency plans include risk assessments and coverage of executive software, computer hardware, and facilities equipment.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)/Department of Defense Chief Information Officer (ASD[C3I]) concurred with the recommendations. The Deputy Secretary of Defense directed written agreements between DISA and the users of each domain at the July 22, 1998, Year 2000 Steering Committee meeting. The Office of the ASD(C3I) coordinated a policy memorandum from the Secretary of Defense including a statement that funds are not to be obligated for any domain user that has failed to sign explicit test agreements with DISA by October 1, 1998. The Office of the ASD(C3I) will also arrange with DISA for the information necessary to inform the Secretaries of the Military Departments and Defense agencies of domains at risk of not becoming Year 2000 ready. DISA concurred with the findings and recommendations. DISA will establish written agreements with the Central Design Activities, report Year 2000 status by domain internally and to the Office of the Secretary of Defense, and report affected applications and agreement status by domain. DISA will selectively test components of the non-standard operating environment, computer hardware, and facility equipment because time and resource constraints will not allow them to test all products. The Director of DISA will instruct the Defense Megacenters to conduct contingency planning and issue requirements in accordance with the recommendations. A discussion of management comments is in Part I and the complete text is in Part III.

Table of Contents

Executive Summary i

Part I - Evaluation Results

Evaluation Background 2
Evaluation Objectives 4
Finding A. Reporting Year 2000 Status 5
Finding B. Testing Year 2000 Compliance 11
Finding C. Planning Year 2000 Contingencies 14

Part II - Additional Information

Appendix A. Evaluation Process
Scope and Methodology 20
Summary of Prior Coverage 21
Appendix B. Glossary 22
Appendix C. Report Distribution 24

Part III - Management Comments

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)/Department of Defense Chief Information Officer Comments 28
Defense Information Systems Agency Comments 32

Part I - Evaluation Results

Evaluation Background

The year 2000 (Y2K) 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, to conserve on electronic data storage and reduce operating costs. Using a two-digit format makes twenty-first century years indistinguishable from those in the twentieth century, thus the year 2000 is identical to 1900, or 2001 to 1901. As a result of this ambiguity, system and application programs that use dates to perform calculations, comparisons, or sorting could generate incorrect results when working with years after 1999.

In addition, the year 2000 is a leap year, the first century leap year since 1600. This means that computer systems and applications must recognize February 29, 2000, as a valid date.

Because of the potential failure of computers to function throughout the Government, the President issued an executive order, "Year 2000 Conversion," dated February 4, 1998, making it policy that Federal agencies ensure that no critical Federal program is disrupted because of the Y2K problem. Also, the head of each agency must ensure that efforts to address the Y2K problem receive the highest priority attention in the agency. The General Accounting Office has designated resolution of the Y2K problem as a high-risk area. DoD has recognized the Y2K issue as critical and has designated it as a material management control weakness area in the FY 1997 Annual Statement of Assurance.

Impact on DoD. As of May 1998, the DoD reported 2,803 mission critical systems. DoD reports indicate that of these systems 480 are Y2K compliant, 255 are scheduled to be replaced, 1,898 are being repaired, and 170 are being retired. The total cost of the DoD Y2K effort was estimated at about $1.93 billion.

DoD Year 2000 Management Strategy. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD[C3I]) issued the "Department of Defense Year 2000 Management Plan" in April 1997. The management plan provides the overall DoD strategy and guidance for inventorying systems, prioritizing systems, retiring systems, and monitoring progress. According to the management plan, the DoD Chief Information Officer has overall responsibility for overseeing the DoD solution to the Y2K problem. DoD Components are responsible for conducting five-phase correction programs: awareness, assessments, renovations, validations, and implementation. In a memorandum for the heads of executive departments and agencies, dated January 20, 1998, the Office of Management and Budget established a new target date of March 1999 for implementing solutions to all systems. Also, the DoD Year 2000 Management Plan is being updated to accelerate the target completion dates for the renovation, validation, and implementation phases. The new mission critical systems target completion date for the renovation phase is August 1998, and the target for completion of all phases is set for December 1998.

Defense Information Systems Agency Roles and Functions. The Defense Information Systems Agency (DISA) is the central manager for major portions of the Defense Information Infrastructure. DISA is responsible for planning, developing, and supporting Command, Control, Communications, Computers, and Intelligence. DISA is subject to the direction, authority, guidance, and control of the ASD(C3I).

DISA WESTHEM. DISA Western Hemisphere (DISA WESTHEM) is the DISA commander's representative for executing the DISA mission within the Western Hemisphere Theater. DISA WESTHEM represents DISA for all functional users who subscribe to the full spectrum of services provided by DISA.
DISA WESTHEM also is responsible for managing the DISA-wide base level information architecture and information systems.

DISA WESTHEM Megacenters. Part of the DISA WESTHEM responsibility is to operate 16 computer processing activities, called Defense Megacenters (DMCs). The DMCs sell mainframe computer processing service to functional users. The functional user's mainframe computer processing service is contained in a logical partition called a "domain." The DMCs are responsible for the Y2K compliance of the computer hardware and the executive software. Concurrently with the Y2K conversion, the DMCs are to be consolidated into six locations under a restructuring to take place during a 14-month period beginning in April 1998. The restructuring will further strain the DMC programming resources.

The DISA WESTHEM responsibility for executive software is exercised through several field commands as well as DMCs. The DISA Support Activity Denver (DSA-D) is responsible for reporting the status of Y2K compliance of the executive software to DISA WESTHEM. The System Support Office (SSO) has offices in Mechanicsburg, Pennsylvania; Montgomery, Alabama; and Dayton, Ohio. The SSO develops and supports the Standard Operating Environment (SOE) and distributes it to the DMCs.

Central Design Activities. Central Design Activities (CDAs) develop and maintain application software. The CDAs are organizationally part of Military Departments and Defense agencies, not DISA WESTHEM. The CDAs are responsible for making the application software work within a domain running at DMCs. When CDAs require additional software utilities for use with application software, the DMCs do the installation. CDAs can require that the DMCs maintain "downlevel" versions of certain executive software utilities. These utilities may not be Y2K compliant but are needed to support the CDA applications. However, these requirements add to the complexity of the DMCs management responsibilities, since the Centers must coordinate changes to executive software with all of the respective CDAs.

Evaluation Objectives

The objective of the evaluation was to determine the adequacy of the Defense Information Systems Agency Year 2000 program with emphasis on the executive software. We evaluated whether the Defense Information Systems Agency's Megacenters have completed adequate planning in accordance with DoD Year 2000 Management Plan guidance. Another objective was to determine whether the progress in making the conversion will meet DoD goals. See Appendix A for a discussion of the evaluation scope and methodology.

Finding A. Reporting Year 2000 Status

The Defense Information Systems Agency Western Hemisphere status reports on the Year 2000 conversion of the executive software needed to process mission critical applications are incomplete and could be misinterpreted. A complete and accurate status reporting is lacking because of the reporting metrics used. The reports did identify that the executive software by product inventory was 60 percent compliant. However, the reports did not reveal that the domain compliance is zero percent. As a result, DoD is at risk of classifying mission critical systems on mainframe computers as being Year 2000 compliant when in fact they are not.

DoD Mission Critical Systems

The DoD Year 2000 Management Plan states that a system is mission critical if the using organization realizes a loss of core capability when the system's capabilities are degraded.

DoD Year 2000 Management Plan Requirements. The Department of Defense Year 2000 Management Plan defines its scope as applying to all organizations in DoD including Defense agencies such as DISA and:

> . . . all systems supported by information technology, including their technical environment, and supporting communication devices, including but not limited to automated business information systems, automated command and control systems, and weapon systems. Information technology support includes hardware, firmware, commercial off the shelf (COTS), Government off the shelf (GOTS) developed software, and data. Software includes COTS/GOTS packages, operating systems, third and forth generation language compilers and interpreters, functional applications, system utilities, translators, and database management systems.

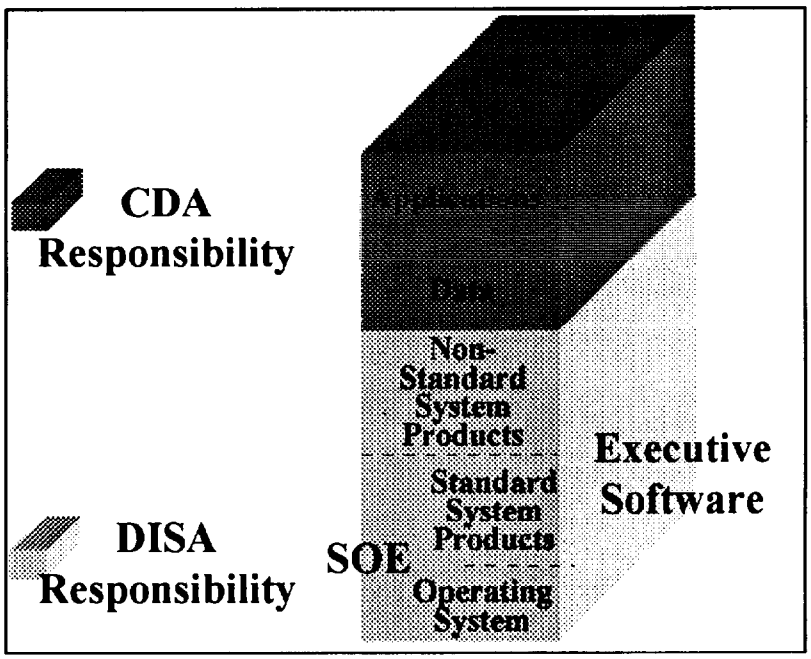
The DoD Year 2000 Management Plan requires the reporting of all systems, which meet or exceed the following criteria:

- a mission critical system;
- a migration system;
- a legacy system;
- a system with a $2M total cost per year . . . ; or
- a system that interfaces with a system that meets any of the above criteria.

Software. The systems that run on a mainframe computer operate in a logical partition called a "domain." The domain includes the application, its data, and the

executive software. The executive software includes the operating system, all of the standard system products, and any other non-standard system products needed by the application. The operating system and a suite of standard system products are called the Standard Operating Environment (SOE). The SOE is furnished by the DISA SSO for use in supporting application production and test domains. The operating system controls the execution of software in the domain and provides services such as resource allocation, scheduling, in-put/out-put control, and data management. The system products provide additional system services, such as data base management. The following figure shows the software elements making up a domain.

The elements of a domain



Reporting Year 2000 Status

Reporting to the Office of Management and Budget. The Office of the Secretary of Defense (OSD) provides quarterly reports on Y2K compliance to the Office of Management and Budget. The reports include a line for DISA Y2K compliance status. For May 1998, the report showed that DISA had 60 mission critical systems, 7 of which were reported Year 2000 compliant. The DMCs were simply one of the 60 systems.

Internal Reporting by DISA. The DISA WESTHEM has been reporting its Y2K status to DISA Headquarters by the number of unique products and the

percentage of these products that are Y2K ready. The DMCs have completed inventorying executive software products. The table provides an extract of mainframe conversion status from a current report to DISA.

DISA WESTHEM Reported Status for April 1998

Mission Critical Item	Number of Items	Percent Y2K Ready	Target Completion Date
Mainframe IBM[1]	45	98	Sep 98
Mainframe Unisys	80	90	Sep 98
Executive Software	2000	60	Sep 98
Mission Support Item			
Facilities Equipment	1499	51	Dec 98

The DMCs provide spreadsheets to DISA WESTHEM containing data on the Y2K compliance of products running within their domains. For those products which are non-Y2K compliant, the DMCs attempt to determine whether a compliant version of the product exists. The compliant product version number is contained in the non-compliant product spreadsheet record.

Adequacy of Year 2000 Status Reporting

OSD Reporting. OSD reports to the Office of Management and Budget do not reflect the status of DMC domains. DMC domain status is fundamental to most DoD mainframe system compliance.

Internal DISA reports. Our analysis of the detailed Y2K status from DISA WESTHEM sites visited showed that none of their domains had completed renovation because all had some executive software Y2K changes to be made. In all IBM domains, the executive software was still in the assessment phase. Each domain had some executive software system products of unknown Y2K status. On the Unisys side, each Air Force domain needed the same small number of known executive software product changes. Each Army and Navy Unisys domain needed CDA action before non-Y2K ready executive software products can be removed.

The variety of executive software conditions included:

- non-Y2K ready operating systems;
- Y2K ready operating systems with system products of unknown vendor or unknown Y2K status;
- Y2K ready operating systems with some Y2K ready system products and others scheduled to be upgraded to Y2K ready versions; and

[1] International Business Machines.

- Y2K ready operating systems with Y2K ready system products but with duplicate non-Y2K ready system products still in use.

The status of actually replacing the non-compliant software is the key to determining Y2K status, not just the availability of replacement software, which is the metric currently used to report the mission critical executive software status. The replacement, however, must be a joint and coordinated effort by both the DMC and the CDA. The need for written agreements between the DMCs and the CDAs is similar to the need for written agreements between system data exchange partners.

The status of coordination plans, schedules, and replacements of non-compliant Y2K executive software is not reported. Therefore, the Y2K reports are incomplete and misleading. Based on our analysis, no mission critical DMC mainframe system is Y2K compliant because their executive software is not Y2K ready. Because of the significance of the DMC domains, it is very important to have the Secretaries of the Military Departments and Defense agencies notified of domains that have high risk of not becoming Y2K ready.

Year 2000 status reporting was also the subject of Inspector General, DoD, Report No. 98-147, "Year 2000 Certification of Mission-Critical DoD Information Technology Systems," June 5, 1998. In that report we indicated that DoD Components were not complying with Y2K certification criteria before reporting that systems are compliant. As a result, DoD reported systems as Y2K compliant that had not been certified or had been certified without justification.

Inspector General, DoD, Report No. 98-184, "Management of the Defense Information Systems Agency Year 2000 Program," August 4, 1998, addressed other weaknesses in the DISA Y2K program.

Consequences of Inaccurate Year 2000 Status Reporting

The information reported by DISA WESTHEM to DISA would lead to the assumption that the DMCs are in the renovation phase and progressing on schedule. However, the reports do not consider the joint work necessary for the domain to be renovated, tested, and implemented. Relying on such inadequate metrics and reports places mission critical applications at risk because a significant amount of conversion work, the coordinated changes between DISA WESTHEM and the CDAs, are not visible for management review. As a result, DoD is at risk of classifying mission critical systems on mainframe computers as being Year 2000 compliant when in fact they are not. The compliance of the DMC domains is fundamental to the compliance of mainframe systems in the Military Departments and Defense agencies.

DISA WESTHEM officials agreed with the importance of domain status to Y2K conversion. They are planning to start reporting actual domain executive software status to DISA.

Summary

Although DISA WESTHEM made measurable progress in pursuing Y2K readiness, no DMC domains were Y2K compliant because their executive software was not Y2K ready. DISA WESTHEM status reports were incomplete and overly optimistic because they concentrated on the availability of Y2K compliant products rather than the status of replacing the non-compliant products in each production domain. Although DISA WESTHEM and the CDAs have joint responsibility for fixing segments of the domains, they have not coordinated their schedules and efforts in either solving or reporting their Y2K problems. As a result, DISA WESTHEM reports did not reasonably state the amount of conversion work to be done and did not provide visibility of the issues blocking progress.

Recommendations, Management Comments, and Evaluation Response

A.1. We recommend that the Department of Defense Chief Information Officer, in conjunction with the Chief Information Officers of the Military Departments and Defense agencies, direct the Central Design Activities to expedite the establishment of written agreements with the Defense Megacenters and Systems Support Office for domain executive software Year 2000 renovation.

ASD(C3I) Comments. The Office of the ASD(C3I) concurred and at the July 22, 1998, Year 2000 Steering Committee meeting, the Deputy Secretary of Defense directed written agreements between DISA and domain users. The Office of the ASD(C3I) coordinated a Secretary of Defense memorandum including a statement that funds are not to be obligated for any domain user that has failed to sign explicit test agreements with DISA by October 1, 1998. The memorandum, dated August 7, 1998, also states that DISA shall provide a report to the Office of the ASD(C3I) by October 15, 1998, listing all domain users who have failed to sign test agreements with DISA by October 1, 1998.

A.2. We recommend that the Director, Defense Information Systems Agency, direct the Defense Megacenters and Systems Support Office to:

a. Establish written agreements with the Central Design Activities and Defense Megacenters to include specific plans and agreements for domain executive software Year 2000 renovations.

b. Report complete Y2K status, including the executive software renovations by domain, for inclusion in Defense Information Systems Agency Western Hemisphere reports to Defense Information Systems Agency Headquarters.

c. Report the applications that are affected by domain, and the status of the coordinated agreements and schedules with the Central Design Activities, for inclusion in Defense Information Systems Agency Western Hemisphere reports to Defense Information Systems Agency Headquarters.

DISA Comments. DISA concurred with the recommendation. DISA was to establish agreements by September 18, 1998, report Y2K status by domain by August 17, 1998, and report the affected applications by domain by August 17, 1998.

A.3. We recommend that the Director, Defense Information Systems Agency, report the domain Year 2000 compliance status to the Office of the Secretary of Defense.

ASD(C3I) Comments. The Office of the ASD(C3I) concurred and will arrange with DISA to obtain the information.

DISA Comments. DISA concurred and was to report domain Year 2000 compliance status to OSD by August 21, 1998.

A.4. We recommend that the Department of Defense Chief Information Officer advise the Secretaries of the Military Departments and Defense agencies when Defense Megacenters identify domains that have high risk of not becoming Year 2000 ready.

ASD(C3I) Comments. The Office of the ASD(C3I) concurred and will request that the Year 2000 compliance reports from DISA include items that would identify domains, mission critical systems, or national security systems that have a high risk of not becoming Year 2000 ready.

Finding B. Testing Year 2000 Compliance

The Defense Information Systems Agency Western Hemisphere planned to comprehensively test the Standard Operating Environment for Year 2000 compliance, but not the non-Standard Operating Environment software, computer hardware, and facility equipment. System programmers and hardware personnel had not been assigned testing responsibilities. The Defense Information Systems Agency Western Hemisphere had not planned testing because of reliance on vendor designation of Y2K readiness and Central Design Activity application testing to test executive software. As a result, mission critical processing may be at risk of date related failures.

Year 2000 Testing Guidance

DoD Year 2000 Management Plan. The DoD Year 2000 Management Plan specifies that:

> The DoD Components must not only test Y2K compliance of individual applications, but also the complex interactions between scores of converted or replaced computer platforms, operating systems, utilities, applications, databases, and interfaces.
>
> All converted or replaced system components must be thoroughly validated and tested to (1) uncover errors introduced during the Renovation Phase, (2) validate Y2K compliance, and (3) verify operational readiness.

DISA Requirement. In the Annex to the DoD Year 2000 Management Plan, DISA requires the validation of all hardware and software before CDA testing. Also, the draft Hardware and Executive Software Test Planning and Validation Development Guide (the Guide) provides a test planning process, basic requirements, criteria, compliance considerations, and an evaluation checklist. Neither the Annex nor the Guide address the testing of facility equipment to ensure Y2K readiness. DISA WESTHEM has not directed the DMCs to implement a software or hardware testing methodology at the time of the evaluation.

Planned Year 2000 Testing

The DISA SSO plans to test the Unisys SOE and the International Business Machines (IBM) SOE. The SSO has contracted with the Defense Continuity of Operations Test Facility, Slidell, Louisiana, to independently test the OS/390 SOE for Y2K compliance. The OS/390 SOE Release 2 or higher is required for the domain to be Y2K compliant. The SSO has scheduled the OS/390 SOE to complete testing by August 21, 1998.

The Montgomery, Alabama, SSO plans to test the Unisys SOE and certify the individual product groups of the Unisys SOE including the operating system, SB5R4. All but 2 platforms managed by the SSO have the SOE installed. The two platforms host Army systems. One of the systems has been "patched" for Y2K compliance as designated by the vendor.

Non-Standard Executive Software, Computer Hardware, and Facility Equipment Testing

Non-standard executive software consists of utilities placed in the domains by the DMCs on behalf of the CDAs.

Neither DISA WESTHEM nor the DMCs have implemented the draft development guide for testing the computer hardware and non-standard executive software at the time of our evaluation. DISA did not provide guidance on testing the facility equipment for Y2K readiness. None of the DMCs had assigned system programmers to testing non-standard executive software, nor had the DMCs allocated personnel for hardware Y2K testing.

Non-Standard Executive Software. The DMCs are responsible for the Y2K compliance of domain specific non-standard software that is not part of the SOE. Although the software product may be used by more than one DMC, no plan currently exists for DISA WESTHEM to manage and report the testing. At the time of our evaluation, the DMCs were depending on vendor designation of Y2K compliance instead of testing the executive software products. The DMCs were also relying on the CDA testing to exercise the executive software in the domain.

Computer Hardware. DSA-D and the SSO Montgomery reported the computer hardware status with respect to vendor designation. Renovation of non-ready computer equipment had been established, but no testing had been planned to validate the vendor's renovation effort.

Facility Equipment. At the time of our evaluation, none of the DMCs visited had plans for testing the facility equipment. The DMCs were responding to taskings from DSA-D to identify all facility equipment and update the Aperture Database. The DMCs did not know whether equipment validation would be handled centrally by DSA-D or whether each DMC would validate their equipment, even for common facility equipment at more than one DMC. Some of the DMCs visited had already initiated Y2K assessment status and were depending on vendor designation of Y2K readiness on their equipment.

Analysis of the Defense Megacenters Testing

DISA has made progress in testing important segments of software for which it is responsible. The DISA SSO plans to test the Unisys SOE and have contracted with the DISA Continuity of Operations Test Facility in Slidell, Louisiana, to test the IBM SOE.

As a result of inadequate and delayed guidance, the DMCs have not implemented testing plans. At the time of our evaluation, none of the DMCs we visited had plans for testing non-standard executive software beyond the functional testing to be conducted by the CDAs. As a result, DISA was relying on vendor designation of Y2K compliance as the only means of quality assurance for a significant portion of the software it manages.

DISA is developing a risk mitigation test strategy based on judgmental sampling. Under the DISA strategy, the DMCs and CDAs would be directed to identify and test products determined to be at risk. DISA is planning to conduct site audits of 10 percent of the site inventory. The planned test strategy also provides for testing of high risk computer hardware. DISA is also working on plans to test facility equipment.

Summary

DISA was not in compliance with the DoD Year 2000 Management Plan requirement for testing. Although the draft Hardware and Executive Software Test Planning and Validation Development Guide had been issued, it had not been implemented throughout the organization. The Guide also did not identify facility equipment testing as a requirement. Without guidance or direction (policy), the DMCs did not know what their test responsibility was. DISA WESTHEM did not direct that testing be planned until the draft plan was issued. Where practical, vendor designation of Y2K readiness should not be used in place of validation.

Recommendations, Management Comments, and Evaluation Response

B. We recommend that the Director, Defense Information Systems Agency, direct the Defense Megacenters and Systems Support Office to plan, conduct, and provide progress reports for comprehensive Year 2000 testing of non-standard executive software, computer hardware, and facility equipment.

DISA Comments. DISA concurred with comment. DISA intends to selectively test components of the non-standard executive software, computer hardware, and facility equipment for Year 2000 compliance. Due to time and resource constraints, DISA will not be able to test all of the executive software products in use. They are currently meeting with customers to jointly decide which products will be tested. The estimated completion date is December 31, 1998.

Finding C. Planning Year 2000 Contingencies

During the evaluation, the Defense Information Systems Agency decided to establish contingency plans and issued initial guidance. However, the contingency planning guidance for recovering from executive software, computer hardware and facilities equipment related Year 2000 failures needs to be expanded. Without more comprehensive planning, mission critical systems may not be able to continue operations if Year 2000 failures occur.

Defense Megacenter Contingency Planning

Contingency plans describe the steps an organization would take, including the activation of manual or contract processes, to ensure the continuity of its core business processes when a system failure occurs. Contingency plans allow management and operations personnel to expeditiously deal with unexpected losses of computer systems, infrastructure facilities, and telecommunications networks. They typically involve switching to a back-up processing facility or operating the mission in a degraded mode, using substitute information processing and communication technology and procedures, until the primary system can be restored.

Y2K failures differ from disaster recovery because date malfunctions and renovated version failures may not be correctable by reverting to old versions of the software. With the Y2K problem, there is no working prior system to transfer back to, since all the existing software is non-compliant. Writing Y2K contingency plans is difficult because executive software, computer hardware, and facilities equipment have unique failure characteristics.

Executive Software, Computer Hardware, and Facilities Equipment. For executive software Y2K failures, problems could be complicated by the need to move the executive software and its operating environment to an alternative location. For example, the executive software may not be licensed to operate at the alternative site, or Y2K failures of the executive software may not be covered by software support agreements.

Hardware Y2K failures are complicated by the commonality of hardware configurations within the DMCs. The typical disaster-recovery approach of moving the affected system to another location fails if the other site has the same hardware configuration. If the hardware is the same, a Y2K failure will affect the moved system at other locations as well. Typically, Y2K contingency plans correct the problem where the failure occurred.

Identification of Y2K problems in facilities is more difficult because of the proliferation of date-sensitive microchips in equipment that previously had

been purely mechanical. Aside from obvious facility elements; such as fire control systems and security systems, less visible elements include interfaces with the outside world such as electrical power, water, and sewage systems. Many activities have only begun assessing the impact of Y2K-induced interruptions of basic services.

Importance of Contingency Plans Based on Risk Assessment. It is good practice in software engineering to base contingency planning on risk assessments. Risk assessments are performed to identify risks and estimate their probability and the impact of their occurrence. Risk assessments provide an estimate of damage, loss, or harm that could result from a failure of individual system components. Risk assessments contribute to contingency planning by focusing on potential disruptions to normal processing.

Contingency Planning Requirements

The DoD Year 2000 Management Plan (the Plan) makes contingency planning part of the Y2K conversion process. DoD requires the development of contingency plans in the Assessment Phase of the Y2K conversion process. The Plan directs components to develop realistic contingency plans, including the development of manual or contract procedures, to ensure continuity of their core processes. The Plan also requires the contingency plans to be updated as Y2K conversion progresses.

Risk Assessment Requirements. The approved version of the DoD Year 2000 Management Plan does not mention the need for risk assessments as a precursor to the writing of contingency plans. However, other recognized guidance on Y2K "best practices" stresses the criticality of performing risk assessments as a crucial component of contingency planning. For example, the GAO Exposure Draft on the "Year 2000 Computing Crises: Business Continuity and Contingency Planning" cites risk and impact analysis as being essential in determining the effect of mission-critical information system failures on the viability and operations of agency core business processes.

Validating Contingency Plans. Another key element of "best practices" is the need to validate contingency plans. The GAO Exposure Draft says that the objective of validation is to evaluate whether individual contingency plans are capable of providing the desired level of support to the agency's core business processes and whether the plans can be implemented within a specified period of time.

Defense Information Systems Agency Contingency Planning

Initially DISA did not plan to write contingency plans for its own use, preferring to rely on the CDAs planning. The first DISA Management Plan, written in August 1997, does not mention contingency planning as part of any of the five conversion phases, although the DoD Year 2000 Management Plan advises first writing plans during the Assessment Phase.

However, DISA has recently recognized the need for contingency plans, and in May 1998, issued guidance directing the DMCs to write specific Y2K contingency plans. But the guidance does not impose milestones for when the individual DMCs should have the action plans written.

Analysis of the DISA Approach. The DISA guidance is comprehensive, covering many important considerations in writing plans. The guidance discusses areas such as: operating system software; hardware; facilities; the Y2K help desk; personnel; communications; supplies; reports; applications; and contracts. However, the guidance does not tie the writing of the plans to the necessary risk assessment. Nor does the guidance emphasize the need to validate the plans.

At the time of our evaluation, the DMCs were waiting for DISA to issue its guidance before writing contingency plans. Although the exact timing for writing plans is not definite, the DoD Year 2000 Management Plan states that the first draft contingency plans should be written during the Assessment Phase of Y2K conversion.

Effects on Executive Software, Computer Hardware, and Facilities Equipment. Issuing facilities equipment Y2K contingency plans depended on completion of two milestones: the publication of final guidance from DISA and a completion of a risk assessment. Facilities equipment contingency planning also awaits completion of the equipment inventory.

Hardware and software contingency plans awaited the completion of guidance and a risk assessment But hardware and software plans face a more complex implementation than facilities equipment, since hardware and software may have to be rehosted at another location. Hardware and software inventory is still not complete and resources to support the contingency plans must be identified before they can be obtained. Hardware plans are also complicated by the presence of common configurations within the DMCs.

Also, since risk assessment and plan validation are part of other best practices, they ought to be part of the DISA guidance.

Potential Problem Areas. Because of the complexity and uniqueness of the Y2K problem, identifying all the potential problems may be difficult. For example, visits to several Megacenters showed that building access to the mainframe computer by the system programmers is not being provided. Instead, Megacenter system programmers are located in a separate building from where the mainframe computer operates. If an environmental-related Y2K failure occurs, such as a loss of power, the system programmers could not access the mainframe computer. Contingency planning would account for the programmer's need for workspace within the building containing the mainframe computer. Detailed analysis of the computer hardware, facilities equipment, and executive software may show additional problems similar to these.

Other Considerations. A final element in contingency planning is the need to set trigger mechanisms to ensure that the plans will be executed when required. Best practices dictate that the contingency plans be validated to ensure that they work, and that the plans be updated based on the results of the live validations.

Resources Needed to Support Contingency Plans. The time lag needed to obtain resources was one of the factors that influenced the authors of the DoD Year 2000 Management Plan to advocate the writing of the contingency plans early in the conversion process, during the Assessment Phase. The DMCs need time to obtain supporting resources for execution of the plans. For example, contractors could be placed on retainers in order to fix problems, or plans could be made for rehosting the software at an alternative site. Regardless of the alternatives proposed, the DMCs must ensure that the resources will be available when they are needed.

Summary

Writing Y2K contingency plans at the DMCs for executive software, computer hardware, and facilities equipment will require a major effort in order to ensure continuity of operations of mission critical systems. DISA has recently recognized the need for contingency planning as part of a sound Y2K conversion management program. However, the guidance needs to be revised to require the performance of risk assessments. To ensure completion, DISA needs to provide specific milestone dates to the DMCs for having the plans written.

Recommendations, Management Comments, and Evaluation Response

C. We recommend that Director, Defense Information Systems Agency, direct the Defense Megacenters to conduct contingency planning and that the requirements be issued to the Defense Megacenters. The direction should include:

1. Writing requirements to complete risk assessments.

2. Writing requirements to plan for contingency coverage of executive software, computer hardware, and facilities equipment.

3. Writing requirements to establish contingency planning milestones.

4. Writing requirements to report the status of contingency planning development, and contingency plan validation.

DISA Comments. DISA concurred and will instruct the DMCs to conduct contingency planning. DISA will issue requirements that include those in the recommendation. The estimated completion date is November 2, 1998.

Part II - Additional Information

Appendix A. Evaluation Process

Scope and Methodology

This is one of a series of reports 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 listing of audit projects addressing this issue, see the Y2K webpage on IGNET at http://www.ignet.gov/.

We evaluated executive software running on mainframe computers at DISA Megacenters, including the Y2K readiness of the hardware, peripherals, and facilities used to support the executive software. We visited the three SSO offices in Mechanicsburg, Pennsylvania; Montgomery, Alabama; and Dayton, Ohio. We also visited Megacenters in Mechanicsburg, Pennsylvania; Columbus, Ohio; St. Louis, Missouri; Oklahoma City, Oklahoma; San Antonio, Texas; and Ogden, Utah. These 6 Centers are the ones the other 10 are being consolidated into. We visited three of the "losing" Megacenters at Chambersburg, Pennsylvania; Montgomery, Alabama; and Dayton, Ohio. We also visited the Denver Support Office in Denver, Colorado, and we attended the quarterly CDA Conference in Jacksonville, Florida, in February 1998. Our conclusions reflect the status of DISA conversion plans as of May 4, 1998.

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

- **Objective:** Prepare now for an uncertain future.
- **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key war fighting capabilities.

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 objectives and goals.

- **Information Technology Management Functional Area. Objective:** Become a mission partner. **Goal:** Serve mission information users as customers.
- **Information Technology Management Functional Area. Objective:** Provide services that satisfy customer information needs. **Goal:** Modernize and integrate DoD information infrastructure.
- **Information Technology Management Functional Area. Objective:** Provide services that satisfy customer information needs. **Goal**: Upgrade technology base.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in DoD. This report provides coverage of the Information Management and Technology high-risk area.

Use of Computer Processed Data. We examined computer records from the DISA Aperture Data Base. Nothing came to our attention as the result of our evaluation that caused us to doubt the reliability of the computer processed data.

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

Management Control Program. We did not review the management control program related to the overall evaluation objectives because DoD recognizes the Year 2000 issue as a material management control weakness area in their annual statements of assurance for FYs 1996 and 1997.

Summary of Prior Coverage

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

Appendix B. Glossary

Aperture. DISA name for a configuration management data base used to track Y2K inventory and status.

Application program. A computer program designed to help people perform a certain type of work. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements.

Computer hardware. The physical components of a computer system, including the mainframe processor, and peripherals such as printers, tape silos, and direct access storage devices.

Domain.[1] A logical part of a mainframe computer where software is designed to work.

Downlevel versions of software. Earlier versions or releases of software which may be running in the same executive software domain as later versions.

Executive software. The collective name for all the system software products, including the operating system, that support the application program.

Facilities equipment. Any devices used in the physical plant of a computer installation whose purpose is the maintenance of the operating environment, such as cooling machinery, security monitors, or lighting.

Mainframe computer. Generic term for large computers which characteristically process and store massive volumes of data.

Mission critical system. A system that when its capabilities are degraded, the organization realizes a resulting loss of core capability.

Platform. A domain in Unisys terminology.

OS/390. A standard IBM operating system which is Year 2000 compliant in versions 2.0 or higher.

SB5R4. SB5 is the current Unisys mainframe computer operating system. Release 4 or higher is known to be Y2K compliant.

Standard Operating Environment. A standard suite of system software that is furnished by the Defense Information Systems Agency SSO for use in supporting application production and test domains.

---

[1] In Unisys terminology, domains are called platforms, but we have used the term "domain" throughout for consistency.

Risk assessments. A continuous process performed during all phases of system development to provide an estimate of the damage, loss, or harm that could result from a failure to successfully develop individual system components.

Testing. Actions to determine that the results generated by the information systems and their components are accurate and the systems perform to specifications.

Utilities. Programs designed to perform maintenance work on a system or on system components - for example, a storage backup program, a disk or file recovery program, or a resource editor.

Appendix C. 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)/
  Chief Information Officer, Department of Defense
  DoD Year 2000 Project Officer
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

Auditor General, Department of the Army
Chief Information Officer, Army

Department of the Navy

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

Department of the Air Force

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

Other Defense Organizations

Director, Ballistic Missile Defense Organization
  Chief Information Officer, Ballistic Missile Defense Organization
Director, Defense Advanced Research Projects Agency
  Chief Information Officer, Defense Advanced Research Projects Agency
Director, Defense Commissary Agency
  Chief Information Officer, Defense Commissary Agency
Director, Defense Contract Audit Agency
  Chief Information Officer, Defense Contract Audit Agency

Other Defense Organizations (cont'd)

Director, Defense Finance and Accounting Service
  Chief Information Officer, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
Director, Defense Legal Services Agency
  Chief Information Officer, Defense Legal Services Agency
Director, Defense Logistics Agency
  Chief Information Officer, Defense Logistics Agency
Director, Defense Security Assistance Agency
  Chief Information Officer, Defense Security Assistance Agency
Director, Defense Security Service
  Chief Information Officer, Defense Security Service
Director, Defense Special Weapons Agency
  Chief Information Officer, Defense Special Weapons Agency
Director, National Security Agency
  Inspector General, National Security Agency
Director, On Site Inspection Agency
  Chief Information Officer, On Site Inspection Agency
Director, Washington Headquarters Services
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency

Non-Defense Federal Organizations and Individuals

Chief Information Officer, General Services Administration
Office of Management and Budget
  Office of Information and Regulatory Affairs
Technical Information Center, National Security and International Affairs Division, General Accounting Office

Chairman and ranking minority member of each of the following congressional committees and subcommittees:

  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 National Security, Committee on Appropriations
  House Committee on Governmental Reform and Oversight
  House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and Oversight
  House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform and Oversight
  House Committee on National Security

Part III - Management Comments

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)/ Department of Defense Chief Information Officer Comments

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

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

August 14, 1998

MEMORANDUM FOR DIRECTOR, ANALYSIS, PLNNNG, AND TECHNICAL SUPPORT DIRECTORATE, INSPECTOR GENERAL, DOD

SUBJECT: Evaluation of the Defense Megacenters Year 2000 Program (Project No. 8PT-3005)

Thank you for providing the outstanding draft report for comment. This report provides unprecedented insight into the interagency relationships involved in the Defense Megacenters Year 2000 (Y2K) Program and their users. The techniques developed by your staff and advocated in the report form a template for solving the problems that have resulted from the lack of interagency agreements for each megacenter domain. We also appreciate the briefing on the report provided by Mr. Ken Stavenjord of your staff to the Y2K Steering Committee on July 22, 1998. This briefing, and the subsequent one by the Director of the Defense Information Systems Agency (DISA), have led to decisions by the Deputy Secretary of Defense at the Y2K Steering Committee meeting to ensure Y2K compliance for all domains. The DoD Chief Information Officer (CIO) staff coordinated a Secretary of Defense memorandum (Attachment 1) to formalize these decisions.

We concur with all the recommendations found in the report. Our comments on the three recommendations that pertain to the DoD CIO at attachment 2.

Should you have any questions, my point of contact for this action is Ms. Sally Brown, 703-602-0967, email: sally.brown@osd.pentagon.mil.

Marvin J. Langston
Deputy Assistant Secretary of Defense
(CIO Policy and Implementation)

Attachments

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)/ Department of Defense Chief Information Officer Comments

THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

7 AUG 1998

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Year 2000 Compliance

The Department of Defense (DoD) is making insufficient progress in its efforts to solve its Y2K computer problem. To improve the accountability for corrective actions, I am directing the following activities in addition to those already underway in this area.

I have asked the Chairman of the Joint Chiefs of Staff to develop a Joint Y2K operational evaluation program and he will give me his plans by October 1, 1998. Starting with their next quarterly reports to me, each of the Unified Commanders-in-Chief will review the status of Y2K implementation within his command and the command of subordinate components. Additionally, starting with the September 1998 Senior Readiness Oversight Council (SROC), the SROC will report on the readiness implications of Y2K.

By September 15, 1998, the Commander-in-Chief of the U.S. Strategic Command, the Senior Civilian Official (SCO) of the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (OASD(C3I)), and the Joint Staff Director of Operations (J-3) will provide to me a detailed report on the Y2K compliance of the nuclear command and control system. This report will be briefed to the DoD Y2K Steering Committee in September.

By October 1, 1998, the Services and Defense Agencies will each report to me on every Acquisition Category (ACAT) I, ACAT IA, and ACAT II system within their purview. Each report will address Y2K compliance or areas of noncompliance of each respective system, to include all related logistics and support systems. Each report will be co-signed by each respective program manager and Program Executive Officer or system command

U13319. /98

commander. This includes the Reserve and National Guard components. Reports will include corrective action plans for Y2K compliance.

The Military Departments, CINCs, and Defense Agencies will be responsible for ensuring that effective October 1, 1998:

(1) The list of mission-critical systems under his or her respective purview is accurately reported in the DoD Y2K database, with each change in mission-critical designation reported and explained within one month of the change to the OASD(C3I).

(2) Funds are not obligated for any mission-critical system that is listed in the Y2K database that lacks a complete set of formal interface agreements for Y2K compliance.

(3) Funds are not obligated for any contract that is for information technology (IT) or national security system (NSS) that processes date-related information and that does not contain Y2K requirements specified in Section 39.106 of the Federal Acquisition Regulation.

(4) Funds are not obligated for any domain user in a Defense Information Systems Agency (DISA) megacenter if that domain user has failed to sign all associated explicit test agreements with DISA.

DISA will provide a report to the OASD(C3I) by October 15, 1998, listing all megacenter domain users who have failed to sign explicit test agreements with DISA by October 1, 1998. Based on OASD(C3I) recommendations, OUSD(Comptroller) (OUSD(C)) will place domain user funds on withhold.

The OUSD(C) will issue guidance to the Military Departments and Defense Agencies on the funding prohibitions described above before October 1, 1998. Program managers for IT or NSS with critical funding needs may seek a waiver from these funding prohibitions. The SCO of the OASD(C3I) may grant waivers to allow funding on a case-by-case basis.

We will take a hard look at progress in November and December. If we are still lagging behind, all further modification to software, except those needed for Y2K remediation, will be prohibited after January 1, 1999.

I ask for your personal, priority involvement as we address this critical national defense issue.

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)/ Department of Defense Chief Information Officer Comments

OASD(C3I) Comments on Recommendations Pertaining to the Office of the Secretary of Defense Draft Evaluation Report, Project No. 8PT-3005, June 29, 1998
Evaluation of the Defense Megacenters Year 2000 Program

A.1. We recommend that the Department of Defense Chief Information Officer, in conjunction with the Chief Information Officers of the Military Services and Defense agencies, direct the Central Design Activities to expedite the establishment of written agreements with the Defense Megacenters and Systems Support Offices for domain executive software Year 2000 renovation:

OASD(C3I) Response: Concur. At the July 22, 1998, Year 2000 Steering Committee meeting, the Deputy Secretary of Defense directed written agreements between the Defense Information Systems Agency and the users of each domain. The staff of the OASD(C3I) is coordinating a policy memorandum at the request of the Deputy Secretary of Defense to formalize the requirements for these agreements.

A.3. We recommend that the Director, Defense Information systems Agency report the domain Year 2000 compliance status to the Office of the Secretary of Defense.

OASD(C3I) Response: Concur. We will arrange with DISA for obtaining this information.

A.4. We recommend that the Department of Defense Chief Information Officer advise the Secretaries of the Military Services and Defense agencies when Defense Megacenters identify domains that have high risk of not becoming Year 2000 ready.

OASD(C3I) Response: Concur. We will request that the Year 2000 compliance status reports be submitted to the OASD(C3I) include items reported to DISA that would

- Identify any mission critical information technology or national security systems as being at high risk of not becoming Year 2000 ready, or
- Identify any domains that have high risk of not becoming Year 2000 ready.

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY REFER TO:

Inspector General

4 August 1998

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Director, APTS Directorate

SUBJECT: Comments to DODIG Draft Audit Report on the Defense Megacenters Year 2000 Program

Reference: DODIG Draft of a Proposed Evaluation Report, Evaluation of the Defense Megacenters Year 2000 Program (Project No. 8PT-3005)

1. We have reviewed the subject draft report and concur with the findings and recommendations. DISA has already begun incorporating the appropriate changes into the DMC Year 2000 Program. The evaluation results indicate that..."although much progress has been made in converting the Defense Megacenter Systems to Year 2000 compliance, problems remain in three areas: reporting, testing, and contingency planning." The enclosure addresses those concerns.

2. The Year 2000 (Y2K) problem continues to be the Director's top priority. The Director has maintained a high focus on the Defense Megacenters, and their approach to achieving Y2K compliant platforms. During the weekly Y2K meetings, chaired by the Vice Director, the DMCs are highlighted to focus on the complexities involved in certifying all domains.

3. The WESTHEM POC for this action is Colonel George Fiedler, USAF, Chief, WESTHEM Operations. He can be contacted at (703) 681-2271 or by email at fiedlerg@ncr.disa.mil. The DISA OIG contact is Ms. Sandra J. Sinkavitch. She can be reached on (703) 607-6316 or by email at sinkavis@ncr.disa.mil.

FOR THE DIRECTOR:

1 Enclosure a/s

RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

MANAGEMENT COMMENTS TO DODIG DRAFT EVALUATION OF THE DISA DEFESE MEGACENTERS YEAR 2000 PROGRAM (Project No. 8PT-3005)

Finding A - Reporting of Year 2000 Status

Recommendation A.2 - Recommend the Director, Defense Information Systems Agency (DISA), direct the Defense Megacenters (DMC) and Systems Support Offices to:

a. Establish written agreements with the Central Design Activities (CDA) and DMCs to include specific plans and agreements for domain executive software Year 2000 renovations.

Response: Concur. DISA will establish the agreements by 18 September 1998.

b. Report complete Y2K status, including the executive software renovations by domain, for inclusion in the DISA WESTHEM reports to DISA Headquarters.

Response: Concur. DISA will report the Y2K status by 17 August 1998.

c. Report the applications that are affected by domain, and the status of the coordinated agreements and schedules with the CDAs, for inclusion in DISA WESTHEM reports to DISA Headquarters.

Response: Concur. DISA will report the affected domains by 17 August 1998.

Recommendation A.3 - Recommend that the Director, DISA, report the domain Year 2000 compliance status to the Office of the Secretary of Defense.

Response: Concur. DISA will report the domain Year 2000 compliance status to OSD by 21 August 1998. As recommended in the evaluation report, DISA will begin to track metrics for the number of domains that are Y2K compliant versus the number of copies of Y2K compliant executive software. In addition DISA will also continue coordinating test schedules with the CDAs to ensure that the Y2K compliant applications can run on certified DMC platforms.

Finding B - Testing Year 2000 Compliance

Recommendation B - Recommend that the Director, DISA, direct the DMCs and Systems Support Officers to plan, conduct, and provide progress reports for comprehensive Year 2000 testing of non-standard executive software, computer hardware, and facility equipment.

Response: Concur with comment. DISA intends to selectively test components of the non-standard operating environment, computer hardware, and facility equipment for Year 2000 compliance. Due to time and resource constraints, DISA will not be able to test all 3000

executive software products currently in use. This agency is currently conducting meetings with its customers to discuss and identify which non-SOE products will be tested/validated independently. Decisions will be made jointly as to which products will be tested. All actions will be formally documented for review. The estimated completion date is 31 December 1998.

Finding C – Planning Year 2000 Contingencies

Recommendation C.1 - Recommend that the Director, DISA, direct the DMCs to conduct contingency planning and that the requirements be issued to the DMCs. The direction should include:

1. Writing requirements to complete risk assessments.
2. Writing requirements to plan for contingency coverage of executive software, computer hardware, and facilities equipment.
3. Writing requirements to establish contingency planning milestones.
4. Writing requirements to report the status of contingency planning development, and contingency plan validation.

Response: Concur. The Director will instruct the DMCs to conduct contingency planning and issue requirements to the DMCs according to the above guidance. The estimated completion date is 2 November 1998.

Evaluation Team Members

The Analysis, Planning, and Technical Support Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report.

Michael G. Huston
Kenneth H. Stavenjord
Danny B. Convis
Jaime A. Bobbio
Wei K. Chang
George B. Cherry