Audit Report

U.S. CENTRAL COMMAND YEAR 2000 ISSUES

Report No. 98-173 July 2, 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 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 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 Audit 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

CENTCOM	U.S. Central Command
Y2K	Year 2000

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

July 2, 1998

MEMORANDUM FOR COMMANDER IN CHIEF, U.S. CENTRAL COMMAND
DIRECTOR, JOINT STAFF

SUBJECT: Audit Report on U.S. Central Command Year 2000 Issues
(Report No. 98-173)

We are providing this report for information and use.

We considered management comments on a draft of this report in preparing the final report. Management comments conformed to DoD Directive 7650.3; therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Mary Lu Ugone at (703) 604-9049 (DSN 664-9049) or Ms. Dianna J. Pearson at (703) 604-9063 (DSN 664-9063). See Appendix C for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-173 **July 2, 1998**
(Project No. 8AS-0006.01)

U.S. Central Command Year 2000 Issues

Executive Summary

Introduction. This report is one in 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. For a listing of audit projects addressing this issue, see the year 2000 webpage on IGnet at <http://www.ignet.gov>.

Information technology systems have typically used two digits to represent the year, such as "98" representing 1998, to conserve electronic 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 and associated systems and application programs that use dates to calculate, compare, and sort could generate incorrect results when working with years after 1999.

Audit Objectives. The overall audit objective was to evaluate the status of the U.S. Central Command's progress in resolving the year 2000 computing issue. Our audit focused on the following year 2000 issues: leadership support and awareness, management and resolution strategy, system assessments, prioritization, system interfaces, testing, risk analysis and contingency planning, and support received from responsible Service executive agents.

Audit Results. The U.S. Central Command has recognized the importance of the year 2000 issue and has taken numerous positive actions in addressing the year 2000 problem. The progress that the U.S. Central Command made in resolving the year 2000 computing issue is not complete. Unless the U.S. Central Command, the Joint Staff, the Services, and Defense agencies make further progress, U.S. Central Command faces a high risk that year-2000-related disruptions will impair its mission capabilities. See Part I for details of the audit results.

Summary of Recommendations. We recommend that the Commander in Chief, U.S. Central Command, monitor and implement revisions to the DoD Year 2000 Management Plan; complete the identification of mission-critical supporting systems and system interfaces; research year 2000 compliance of vendor software and test mission-critical vendor software; prepare written interface agreements and develop contingency plans for mission-critical systems that the U.S. Central Command manages; document test plans to show how managed systems were deemed compliant and determine the level of year 2000 compliance; coordinate year 2000 solutions with the Component Commands; and use selected command and joint exercises to test

year 2000 scenarios in an operational environment. We recommend that the Director, Joint Staff, develop an inventory of and assist the unified commands in obtaining year 2000 information on mission-critical supporting systems that Services or other organizations manage; implement procedures to monitor and track the status of mission-critical systems; assist the unified commands in testing systems and applications common to the unified commands; disseminate year 2000 information on commercial off-the-shelf products and Government off-the-shelf products; and use selected joint exercises to test year 2000 scenarios in an operational environment.

Management Comments. The U.S. Central Command and the Joint Staff concurred with the recommendations. See Part I for a summary of management comments and Part III for the complete text of the comments.

Table of Contents

Executive Summary i

Part I - Audit Results

Audit Background 2
Audit Objectives 4
Status of the U.S. Central Command Year 2000 Program 5

Part II - Additional Information

Appendix A. Audit Process
Scope 18
Methodology 19
Prior Audit Coverage 19
Appendix B. Other Matters of Interest 20
Appendix C. Report Distribution 22

Part III - Management Comments

U.S. Central Command Comments 26
Joint Staff Comments 29

Part I - Audit Results

Audit Background

The year 2000 (Y2K) problem is the term most often used to describe the potential failure of information technology systems to process or perform date-related functions before, on, or after the turn of the century. The Y2K problem is rooted in the way that automated information systems record and compute dates. For the past several decades, systems have typically used two digits to represent the year, such as "98" representing 1998, to conserve on electronic data storage and reduce operating costs. With the two-digit format, however, 2000 is indistinguishable from 1900. As a result of the ambiguity, computers and associated systems and application programs that use dates to calculate, compare, or sort could generate incorrect results when working with years following 1999. Calculation of Y2K dates is further complicated because the Y2K is a leap year, the first century leap year since 1600. The computer systems and applications must recognize February 29, 2000, as a valid date.

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

DoD Y2K Management Strategy. In his role as the DoD Chief Information Officer, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued the "DoD Year 2000 Management Plan" (DoD Management Plan) in April 1997. The DoD Management Plan provides the overall DoD strategy and guidance for inventorying, prioritizing, fixing, or retiring systems, and monitoring progress. The DoD Management Plan states that the DoD Chief Information Officer has overall responsibility for overseeing the DoD solution to the Y2K problem. Also, the DoD Management Plan makes the DoD Components responsible for the five-phase Y2K management process, consisting of awareness, assessments, renovations, validations, and implementation actions. The DoD Management Plan includes a description of the five-phase Y2K management process.

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) is in the process of issuing an updated DoD Management Plan, which accelerates the target completion dates for the renovation, validation, and implementation phases.

In a memorandum dated January 20, 1998, for the heads of executive departments and agencies, the Office of Management and Budget established a new target date of March 1999 for implementing corrective actions to all systems. The new target completion dates are September 1998 for the renovation phase and January 1999 for the validation phase.

The Joint Chiefs of Staff. The Chairman of the Joint Chiefs of Staff is the principal military advisor to the President, the Secretary of Defense, and the National Security Council. The Joint Chiefs of Staff have no executive authority to command the combatant forces. The Secretaries of the Military Departments assign all forces under their jurisdiction to the unified commands to perform missions assigned to those commands.

The Joint Staff Director, Command, Control, Communications, and Computer Systems (J6), has been designated by the Chairman of the Joint Chiefs of Staff to oversee the unified commands' and Joint Staff's implementation of the DoD Management Plan.

The Joint Staff. The Joint Staff assists the Chairman of the Joint Chiefs of Staff with unified strategic direction of the combatant forces; unified operation of the combatant commands; and integration into an efficient team of land, naval, and air forces.

Year 2000 Action Plan. The Joint Staff Year 2000 Action Plan provides the unified commands and Joint Staff directorates the corporate strategy and management approach for addressing the Y2K problem. The action plan uses the accelerated target completion dates for the renovation, validation, and implementation phases in the draft DoD Management Plan. The action plan provides that the unified commands should target December 31, 1998, for completion of all Y2K efforts.

U.S. Central Command. The U.S. Central Command (CENTCOM) is one of nine unified commands in the Department of Defense. The CENTCOM was activated on January 1, 1983. The CENTCOM is the administrative headquarters for U.S. military affairs in 20 countries of the Middle East, Southwest Asia, Northeast Africa, and the Arabian Gulf. That region contains more than 70 percent of the world's oil reserves, making it vital to the economies of the United States and its allies. The CENTCOM reports through the Chairman of the Joint Chiefs of Staff to the Secretary of Defense. The overall mission of CENTCOM is to support U.S. and free-world interests by:

- ensuring access to theater oil resources;

- helping friendly regional states to maintain their own security and a collective defense;

- maintaining an effective and visible U.S. military presence in the region; and

- deterring threats from hostile regional states and providing U.S. military force into the region, if necessary.

The CENTCOM is supported by component commands from each Service that provide forces as required to conduct operations. The component commands are the U.S. Army Forces Central Command, the U.S. Naval Forces Central Command, the U.S. Central Command Air Forces, and the Special Operations Command Central Command. Additionally, the Joint Task Force South West Asia and Security Assistance Offices in several nations complement the U.S. military forces in the region by coordinating the efforts of CENTCOM with their respective host nations.

Audit Objectives

The overall audit objective was to evaluate the status of the progress of CENTCOM in resolving its Y2K computing issue. Our audit focused on the following Y2K issues: leadership support and awareness, management and resolution strategy, system assessments, prioritization, system interfaces, testing, risk analysis and contingency planning, and support received from responsible Service executive agents. See Appendix A for a discussion of the audit scope and methodology and summary of prior audit coverage, and Appendix B for other matters of interest.

Status of the U.S. Central Command Year 2000 Program

The CENTCOM has taken several positive actions to address its Y2K problem. However, CENTCOM and the Joint Staff have not completed all of the actions necessary to minimize the adverse impact of Y2K date processing in mission and mission-support systems. Progress is not complete because the Joint Staff needs to compile a comprehensive list of mission-critical supporting systems for all of the unified commands to include the system manager and the status of Y2K compliance. The CENTCOM needs to:

- identify the mission-criticality of all of its supporting systems;

- monitor the Joint Staff unified command supporting systems list and assess the impact to the CENTCOM area of responsibility mission and develop operational contingency plans accordingly;

- determine Y2K compliance of vendor software and test mission-critical commercial off-the-shelf products;

- complete the identification of system interfaces and prepare written interface agreements for mission-critical systems that CENTCOM manages;

- develop contingency plans for CENTCOM-managed mission-critical systems;

- document test plans to show how CENTCOM-managed systems were deemed compliant and determine the level of Y2K compliance;

- coordinate Y2K solutions and contingency plans with its component commands to ensure mission accomplishment; and

- use selected command and joint exercises to test Y2K scenarios in an operational environment.

Unless the CENTCOM, the Joint Staff, the Services, and Defense agencies collectively make further progress, CENTCOM faces a high risk that Y2K-related disruptions will impair its mission capabilities.

Y2K Management Planning, Strategy, and Oversight

Y2K Program Management. The CENTCOM Director of Command and Control, Communications, and Computer Systems (J6) has responsibility for the CENTCOM Year 2000 Program. The Director provides status briefings on Y2K to the Commander-in-Chief on a monthly basis.

The CENTCOM has taken the following actions as part of its efforts to address the Y2K problem:

- prepared the CENTCOM Y2K project plan,
- appointed a Y2K point of contact for all of CENTCOM,
- identified technical and management points of contact for each functional directorate and proponent organization,
- implemented a corporate strategy to solve Y2K problems by implementing the DoD Management Plan, and
- established a CENTCOM Y2K web page.

The CENTCOM Y2K web page makes available various Y2K documents, including the CENTCOM Y2K project plan, the systems inventory database, minutes of the computer support coordinator meetings, and Y2K points of contact.

Y2K Project Plan. The CENTCOM Y2K project plan is intended to provide the overall strategy and actions necessary to accomplish the following:

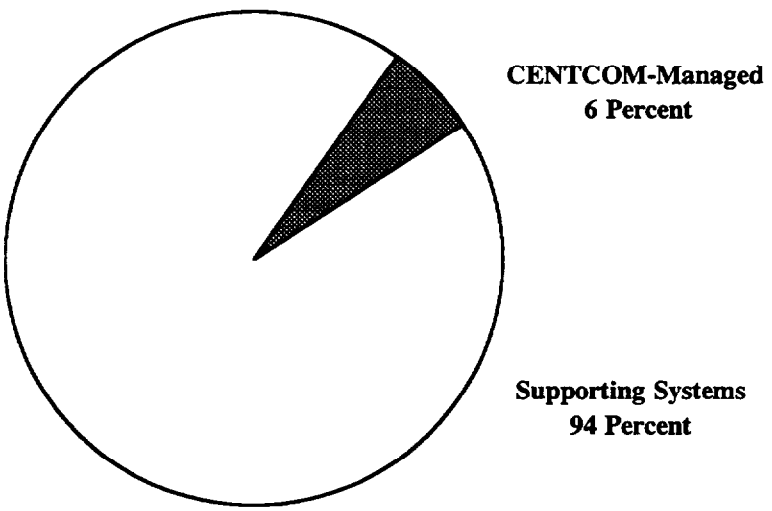
- identify all CENTCOM systems that may be affected by the Y2K problem,
- determine the corrective measures that should be taken, and
- implement those corrective measures.

The project plan is tailored to the DoD Management Plan and is intended to address the Y2K problem by implementing the five phases required by the DoD Management Plan. However, the project plan does not require the CENTCOM to monitor changes to the DoD Management Plan and update its plan based on changes to the DoD Management Plan. Each CENTCOM directorate is to identify a point of contact to carry out the actions called for in the project plan.

Y2K Participation. The CENTCOM addresses Y2K issues at the monthly computer support coordinators meetings. Each CENTCOM directorate and staff organization has a computer support coordinator. The meetings are a forum to discuss and address computer-related issues, including Y2K. Additionally, the Y2K point of contact assigns Y2K taskings to the computer support coordinators.

Identification of Systems

The CENTCOM identified 469 managed and supporting systems and software applications to fulfill its mission and everyday operations. Managed systems are those systems for which CENTCOM has program management responsibility. Supporting systems are those systems that Services or other organizations manage. As of January 1998, CENTCOM identified 15 CENTCOM-managed systems and 235 supporting systems. Additionally, CENTCOM determined that it uses 219 commercial off-the-shelf products. As the following figure indicates, CENTCOM relies heavily on supporting systems.



CENTCOM Inventory of Systems and Software

Systems Inventory. The CENTCOM began developing a list of software and systems in December 1996. From December 1996 through March 1997, the J6 directorate tasked the computer support coordinators to do the following:

- review the command standard and approved software listing for continued use and undocumented software,
- identify any networks and hardware within their directorates,
- identify any systems or software within their directorates,
- identify any systems or software within their directorates provided by outside agencies, and
- inform the Y2K point of contact of potential Y2K problems.

In July 1997, the Director of J6 requested that all CENTCOM directorates and staff offices review the CENTCOM Y2K software and systems listing for accuracy and completeness. In November 1997, the J6 directorate tasked the computer support coordinators to review the CENTCOM systems list and identify interfaces for the systems within their directorate.

The CENTCOM has produced a software and systems inventory spreadsheet, which is available at its Y2K web site. The spreadsheet shows the status of CENTCOM systems to include the following status categories: user, mission-criticality, Y2K compliance, executive agent, Y2K phase, renovation method, interfaces, and point of contact.

As stated, the CENTCOM inventory consists of 469 systems and software applications to fulfill mission and everyday operations. To determine the potential impact of noncompliance of any of the 469 systems and applications, CENTCOM would have to complete its determination of the systems and applications that are mission-critical. The following table provides a breakout of the status of CENTCOM systems as of January 1998.

CENTCOM Systems and Applications

	Mission-Critical			
	Yes	No	Not Stated	Total
CENTCOM-managed systems	9	6	0	15
CENTCOM-supporting systems	66	45	124	235
Commercial off-the-shelf products	19	54	146	219
Total systems and applications	**94**	**105**	**270**	**469**

The J6 directorate made a preliminary determination that 94 systems and applications are critical to the mission of CENTCOM. However, CENTCOM has not determined mission-criticality for 270 supporting systems and commercial off-the-shelf products.

Systems Managed by CENTCOM. The CENTCOM manages 15 systems. The systems can be categorized as the following:

- local area networks,
- electronic mail network,
- personnel locator,
- message processor,
- record of clearance,
- staff suspense system,
- personnel system, and
- update status reports.

The CENTCOM is the owner of the code of 4 of the 15 systems that it manages, and the other 11 systems are systems configured of commercial off-the-shelf products. The CENTCOM is planning to have all of its managed systems tested and compliant, not later than October 1, 1998.

CENTCOM Supporting Systems. The CENTCOM has not identified the mission-criticality and the owners of all its supporting systems. Further, CENTCOM has not determined the status of Y2K compliance of its mission-critical supporting systems. The Joint Staff needs to compile a comprehensive inventory list of mission-critical supporting systems for all of the unified commands to include system manager and status of Y2K compliance. Upon completion of the Joint Staff unified command supporting systems list, CENTCOM needs to monitor and assess the impact to the CENTCOM mission area of responsibility and develop contingency plans accordingly.

We reviewed the Services' and the Defense Information Systems Agency's mission-critical systems lists. As of November 1997, the lists identified only 20 of the 102 supporting systems belonging to the Services and the Defense Information Systems Agency as mission-critical. Further, CENTCOM identified 31 systems as mission-critical that the Services and the Defense Information Systems Agency did not identify as mission-critical. The CENTCOM, with the help of its component commands and the functional directorates, needs to complete the identification of mission-critical supporting systems because the appropriate executive agents need to be aware of the systems that are critical to the CENTCOM mission. After CENTCOM has identified the mission-critical supporting systems, the Joint Staff should assist

CENTCOM and the other unified commands in obtaining Y2K information on mission-critical supporting systems that Services or other organizations manage.

The CENTCOM has identified 235 supporting systems for which Y2K compliance is contingent upon another DoD Component. Of the 235 supporting systems, CENTCOM has identified 66 mission-critical systems, 45 non-mission-critical systems, and 124 systems of which no determination has yet been made as to mission-criticality. The CENTCOM has not defined a method for determining the adverse impact of Y2K date processing in its supporting systems.

The CENTCOM stated that it had identified the owner of all of the systems that CENTCOM presently uses. However, a review of the CENTCOM systems inventory list indicates that CENTCOM has not identified the owner for 154 systems and applications. The CENTCOM needs to complete the identification of the owners of its supporting systems. Further, CENTCOM needs to determine the status of those systems and the mission-criticality placed on those systems.

The CENTCOM has not developed a method for determining the status of those supporting systems critical to its mission and, therefore, cannot determine the impact of supporting system failure on the mission of CENTCOM. The Joint Staff should develop and maintain a comprehensive inventory list of mission-critical supporting systems and implement procedures to monitor and track the status of those mission-critical systems. Those actions would enable CENTCOM and the unified commands to monitor the progress of their supporting systems and to prepare operational contingency plans for their mission areas, accordingly.

Commercial Off-the-Shelf Products. The CENTCOM has not determined Y2K compliance for 203 of 219 of its listed commercial off-the-shelf products. The DoD Management Plan requires that the component not only compile a comprehensive list of vendor software used but also, during the Assessment Phase, determine whether the vendor software is Y2K compliant. The Joint Staff should coordinate with the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in obtaining Y2K information on the Y2K compliance of vendor software and disseminating it to CENTCOM and the unified commands.

Interfaces and Written Interface Agreements

Interfaces. The CENTCOM has not completed identifying system interfaces and preparing written interface agreements. As a result, CENTCOM is unable to determine the status of those interfaces that may impact the mission of CENTCOM. For example, CENTCOM did not identify the Global Command and Control System as a systems interface to the CENTCOM Command and Control network, although the interface exists. The DoD Management Plan states that interfaces involve sending and receiving data among Services,

Defense agencies, or both, or external DoD vendors. Interfaces are critical to the Y2K effort because they have the potential to introduce or propagate errors, or both, from one DoD Component to another. The systems of CENTCOM interface with or connect to many computer systems belonging to the Services, DoD Components, and other organizations. In addition to known interfaces, CENTCOM may interface with systems of allied, coalition, and other Federal agencies. Because those systems are also vulnerable to Y2K problems, they can also introduce or propagate errors, or both, into CENTCOM systems. Timely and complete information on all system interfaces that may be affected by Y2K changes is critical to the success of the Y2K compliance program of CENTCOM. The CENTCOM should complete the identification of system interfaces.

Written Interface Agreements. The DoD Management Plan states that DoD Components need to determine the dependency links between internal and external systems; determine dependency links between core mission areas, processes, and all data exchange entities; and provide for date and data format conversions where necessary. A validation process is necessary to ensure compliance. The sample Y2K compliance checklist in the DoD Management Plan states that DoD Components and each interface partner should negotiate an agreement dealing with Y2K issues. The DoD Components and their interface partners should discuss and verify that they have implemented consistent Y2K corrections for data passed between the systems. The CENTCOM needs to prepare written interface agreements to reduce the risk of discovering too late in the Y2K effort that an interfacing system will not be able to accommodate the agency's own Y2K changes. The interface agreements should provide for the same types of information as in the DoD Management Plan sample Year 2000 Compliance Checklist.

Contingency Plans

The CENTCOM has not developed contingency plans for any of its managed systems. The DoD Management Plan states that DoD Components should develop realistic contingency plans, including the development and activation of manual or contract procedures, to ensure the continuity of core processes. Contingency plans are to be prepared during the assessment phase and should be updated at each successive phase. The CENTCOM stated in its response to an Office of the Inspector General, DoD, questionnaire that it had contingency plans for each mission-critical system in the event that the system fails to pass testing. However, the contingency plans were not documented.

In addition to system contingency plans, CENTCOM should review and assess contingency plans for mission-critical supporting systems, as they become available, and develop operational contingency plans as needed. The Joint Chiefs of Staff Year 2000 Action Plan states that the unified commands are not expected to know detailed information about the mission-critical systems provided by the Services and Defense agencies. However, the unified commands must conduct sufficient planning and establish alternate procedures to successfully complete the organization's mission while the system's program managers and technical staff make necessary year 2000 corrections. The Joint Chiefs of Staff Year 2000 Action Plan provides guidance on developing both operational and system contingency plans.

Testing and Compliance Checklists

The CENTCOM reports that 8 of 15 managed systems are Y2K compliant, and 3 of 9 mission-critical managed systems are Y2K compliant. The CENTCOM had tested and completed compliance checklists for 4 of the 15 managed systems but had not provided documented test plans to show how the systems were deemed compliant.

Testing. The DoD Management Plan states that DoD Components need an extensive period of time to adequately validate and test converted or replaced systems for Y2K compliance. DoD Components not only must test for Y2K compliance of individual applications, but must also test the complex interactions between scores of converted or replaced computer platforms, operating systems, utilities, applications, databases, and interfaces. All converted or replaced system components introduced during the "renovation" phase must be thoroughly validated and tested to uncover errors, validate Y2K compliance, and verify operational readiness. The Joint Staff should assist the unified commands in testing systems and applications common to the unified commands.

The CENTCOM has a general automated data processing contract in place, which can be used for Y2K testing. The Command, Control, Communications, and Computer Systems directorate has a computer laboratory configured for testing personal computer-based systems and limited testing of Sun-based systems or systems operating from a solaris operating environment. Additionally, Combat and Analysis has a computer laboratory setup for testing Sun-based systems.

Compliance Checklists. As stated in this section, the contractor has validated Y2K compliance for 4 of the 15 managed systems; 1 system is mission-critical. The validation process requires the system manager to complete the DoD Management Plan checklist and certify the level of Y2K compliance. Although the contractor has signed the checklists, the contractor has not provided documented test plans. Additionally, the contractor did not certify the level of Y2K compliance for each of the four systems. The CENTCOM has not

identified all the system interfaces that require testing. The CENTCOM should test mission-critical vendor software for Y2K compliance and should document test plans to show how managed systems are Y2K compliant.

The Joint Interoperability Test Command provides general assistance in Y2K resolution that includes test planning, test case development, and solution recommendations. In addition, the Joint Interoperability Test Command can provide specific assistance in support of a system to include analysis of hardware platforms and software application packages, development and execution of a Y2K test plan, recommendations to resolve Y2K impacts, and implementation of resolution recommendations.

Component Commands

The CENTCOM has limited oversight over its component command Y2K problems and solutions, except for interfaces, because the CENTCOM component commands report the Y2K status of those systems through Military Departments. As a result, CENTCOM does not know how the Y2K issues will impact the overall mission of CENTCOM. Because the CENTCOM mission will involve the component commands, the resolution strategy and implementation of that strategy is a dual responsibility of CENTCOM and its component commands. Therefore, CENTCOM should coordinate Y2K solutions and contingency plans with the component commands, in accordance with the DoD Management Plan.

Use of Selected Command and Joint Exercises to Test Y2K Scenarios

The CENTCOM could use selected command and joint exercises to test and measure the extent of potential Y2K problems that face the warfighter and to allow time to correct critical problems. The DoD Management Plan states that testing should take place in a realistic test environment and should account for the interoperability of system interfaces. The use of selected joint exercises to test Y2K scenarios in an operational environment would provide CENTCOM and the other unified commands the opportunity to test and validate systems in a realistic test environment.

Unified command exercises test operational plans, validate force apportionment, support political and military relationships and objectives, and foster regional engagements of unified commanders. Joint exercises include joint training events based on approved joint doctrine that prepares joint forces or staffs to respond to operational requirements established by the combatant commanders to accomplish their assigned missions. Mission focus is critical to the effectiveness and efficiency of joint training exercises. The goals of joint training are to prepare for war, prepare for military operations other than war, prepare for multinational operations, and integrate the interagency process. The

joint exercises focus on plans, policies, procedures, and training required to ensure that senior leaders can effectively direct and integrate U.S. and coalition military forces during war. Common operational joint tasks are activities conducted by or for multiple supported commands under similar conditions and to a common joint standard. The common tasks are selected by multiple combatant commands through the mission analysis process, and they describe a list of core joint competencies that are fundamental to joint operations. The common joint tasks include the following:

- conducting operational movement and maneuvers,
- developing operational intelligence,
- employing operational firepower,
- providing operational support,
- exercising operational command and control, and
- providing operational protection.

Because of time constraints posed by Y2K issues, using selected command and joint exercises to test Y2K scenarios may assist CENTCOM in making further progress to identify and resolve Y2K problems. Inspector General, DoD, Report No. 98-129, "U.S. Special Operations Command Year 2000 Issues," May 8, 1998, recommended that the Joint Staff integrate year 2000 scenarios into operational requirements in joint exercises in FY 1998 for the purposes of determining the extent of potential Y2K impact on the continuity of the warfighter.

The House bill to authorize appropriations for FY 1999 for the Department of Defense, H. R. 3616, proposes that the Secretary of Defense submit to Congress a report containing a plan to include simulated Y2K scenarios in military exercises conducted from January 1, 1999, through September 30, 1999. The plan shall include military exercises conducted under the Chairman of the Joint Chiefs of Staff Exercise Program. Additionally, the plan is to cover systems excluded from the exercise and provide an explanation of how the military exercise will use an excluded system's Y2K contingency plan.

Performing command and joint exercises to test Y2K interoperability of system interdependencies and interfaces may not be possible in some instances if the Services and Defense agencies have not made and implemented the necessary Y2K corrections to the required systems. In such cases, testing contingency plans in an operational environment would be necessary. Testing contingency plans will help CENTCOM assess its capability to continue operations if systems fail because of Y2K problems.

Conclusion

Although CENTCOM has made initial progress, CENTCOM must continue to address several critical issues. The CENTCOM has recognized the importance of solving Y2K problems in systems to reduce the risk of Y2K failure, but CENTCOM must take a more aggressive approach to dealing with Y2K for supporting systems and commercial off-the-shelf products to ensure that it is well-positioned to deal with unexpected problems and delays. Unless the Services and Defense agencies make further progress, CENTCOM faces a high risk that Y2K-related disruptions will impair its mission capabilities. Therefore, CENTCOM must continually monitor and assess the progress of supporting systems and prepare contingency plans for its mission areas, accordingly. A Joint-Staff-prepared composite DoD mission-critical database would greatly facilitate the ability of CENTCOM and the other unified commands to monitor the progress of its supporting systems and prepare contingency plans for its mission areas. Copies of this report are being provided to all unified commands to facilitate self reviews of Y2K efforts.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Commander in Chief, U.S. Central Command:

a. Monitor revisions to the DoD Year 2000 Management Plan and implement the revisions into the U.S. Central Command Year 2000 project plan.

b. Monitor the Joint Staff unified command supporting systems list to determine the status of its supporting systems and assess the impact to the U.S. Central Command area of responsibility mission and develop operational contingency plans accordingly.

c. Complete the identification of mission-critical supporting systems that Services or other organizations manage and the owners of all of its supporting systems.

d. Complete the identification of system interfaces and prepare written interface agreements for mission-critical systems that the U.S. Central Command manages.

e. Develop contingency plans for U.S. Central Command managed mission-critical systems.

f. Review and assess contingency plans for mission-critical supporting systems and develop operational contingency plans as needed.

g. Research year 2000 compliance of vendor software and test mission-critical vendor software for year 2000 compliance.

h. Document test plans to show how managed systems were deemed compliant and determine the level of year 2000 compliance.

i. Coordinate year 2000 solutions and contingency plans with U.S. Central Command component commands.

j. Use selected command and joint exercises to test year 2000 scenarios in an operational environment.

Management Comments. The U.S. Central Command concurred with all of the recommendations, stating progress made and future intentions for each recommendation.

2. We recommend that the Director, Joint Staff:

a. Develop and maintain a comprehensive inventory list of mission-critical supporting systems to enable the unified commands to monitor the progress of the Services and agencies and to assess the impact of mission operations.

b. Assist the unified commands in obtaining year 2000 information on mission-critical supporting systems that Services or other organizations manage.

c. Implement procedures to monitor and track the status of mission-critical supporting systems.

d. Coordinate with the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to obtain and disseminate year 2000 information on commercial off-the-shelf and Government off-the-shelf products.

e. Assist the unified commands in testing systems and applications that are common to the unified commands.

f. Integrate year 2000 scenarios into operational requirements in joint exercises starting in FY 1998 for the purposes of determining the extent of potential year 2000 impact on continuity of warfighter operations.

Management Comments. The Joint Staff concurred with all of the recommendations, stating progress made and future intentions for each recommendation.

Part II - Additional Information

Appendix A. Audit Process

This report is one in 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>.

Scope

We reviewed and evaluated the status of the progress of CENTCOM in resolving the Y2K computing issue. We evaluated the Y2K efforts of CENTCOM, compared with those efforts described in the DoD Management Plan issued by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in April 1997. We obtained documentation including the CENTCOM Y2K project plan, the CENTCOM Y2K responses to the Office of the Inspector General, DoD, Y2K questionnaire, and systems inventory database information as of January 1998. We used the information to assess efforts related to the multiple phases of managing the Y2K problem.

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

- **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-3)**

- **Objective:** Fundamentally reengineer DoD 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 objectives and goals.

- **Information Technology Management Functional Area. Objective:** Become a mission partner. **Goal:** Serve mission information users as customers. **(ITM-1.2)**

- **Information Technology Management Functional Area. Objective:** Provide services that satisfy customer information needs. **Goal:** Modernize and integrate Defense information infrastructure. **(ITM-2.2)**

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

Methodology

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from January through March 1998 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did not use computer-processed data to perform this audit.

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

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness area in the FY 1997 Annual Statement of Assurance.

Prior Audit 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. Other Matters of Interest

External Reporting

The DoD Components are required to provide information to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) on a quarterly basis. The reason for that reporting is to give the visibility necessary to ensure a thorough and successful transition to Y2K compliance for all DoD systems.

Quarterly Report Input. The quarterly report dated January 16, 1998, prepared by the Joint Staff and sent to Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), does not reflect the status of the CENTCOM systems. The CENTCOM reported 15 systems as CENTCOM Y2K reportable systems, 9 of which it identified as critical to its mission. However, the Joint Staff reported 20 CENTCOM systems and reported no systems as mission-critical. Based on the documentation that CENTCOM provided, the Joint Staff should have reported the following to Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) about the CENTCOM mission-critical systems:

Number being replaced	5	
Planned terminations	1	
Number of non-compliant systems	6	
Number of compliant systems		3*
Total number of mission-critical systems		9

*Only one mission-critical system has been certified as Y2K compliant. CENTCOM relied on vendor and in-house certification.

Cost Estimates

The CENTCOM estimates that Y2K compliance will cost $250,000 for testing and implementation of its systems. However, all CENTCOM-managed systems and legacy systems will be made Y2K compliant as part of their normal life-cycle maintenance. The CENTCOM-developed software has been rewritten

as part of the CENTCOM network migration. The CENTCOM does not anticipate additional funding or materials requirements strictly for Y2K compliance.

CENTCOM Areas of Concern

The CENTCOM expressed concern about the systems that are out of its control. The CENTCOM believes that contact with program managers is necessary to determine both Y2K solutions and status. The Joint Staff can provide assistance, especially with those systems and commercial off-the-shelf products common to the unified commands. The CENTCOM suggested that the common operating environment is another area of concern because DoD is constantly changing the common operating environment. The CENTCOM stated that DoD needs to stabilize the operating environment until the Y2K problem has been solved.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Deputy Under Secretary of Defense (Logistics)
  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)
  Year 2000 Oversight and Contingency Planning Office
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
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

Unified Commands

Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Atlantic Command
Commander in Chief, U.S. Southern Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. Space Command
Commander in Chief, U.S. Special Operations Command
Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command

Other Defense Organizations

Director, Defense Contract Audit Agency
  Chief Information Officer, Defense Contract Audit Agency
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
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence 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
Director, Defense Information and Financial Management Systems, Accounting and Information Management 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 Special Committee on the Year 2000 Technology Problem
  Senate Committee on Governmental Affairs
  House Committee on Appropriations
  House Subcommittee on National Security, Committee on Appropriations
  House Committee on Governmental Reform and Oversight

Non-Defense Federal Organizations and Individuals (cont'd)

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

U.S. Central Command Comments

UNITED STATES CENTRAL COMMAND
OFFICE OF THE COMMANDER IN CHIEF
7115 SOUTH BOUNDARY BOULEVARD
MACDILL AIR FORCE BASE, FLORIDA 33621-5101

CCIG

MEMORANDUM THRU DIRECTOR, JOINT STAFF, PENTAGON, WASHINGTON, DC 20318

FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, 400 ARMY NAVY DRIVE, ARLINGTON, VIRGINIA 22202-2884

SUBJECT: Audit Report on U.S. Central Command Year 2000 Issues (Project No. 8AS-0006.01)

1. The failure of my information technology systems would severely degrade my ability to carry out the mission of U.S. Central Command and so I thank you for providing an audit of our efforts to solve the Year 2000 problem. We have reviewed your audit report, concur with the recommendations, and are taking actions to implement those recommendations.

2. Specific comments on your recommendations are enclosed. We remain dedicated to resolving Year 2000 problems with our mission-critical information technology systems. My point of contact for Year 2000 issues is Lt Col Zuzack, CCJ6-DI, at (813) 828-0059, DSN 968-0059.

Encl
as

A.C. Zinni
General, USMC
Commander in Chief

Audit Report on U.S. Central Command Year 2000 Issues (Project No. 8AS-0006.01)

Recommendation a: Monitor revisions to the DoD Year 2000 Management Plan and implement the revisions into the U.S. Central Command Year 2000 project plan.

USCENTCOM Comments: Concur. U.S. Central Command's Year 2000 Project Plan is a living document based on the current DoD Year 2000 Management Plan. Changes to the management plan can easily be incorporated into our project plan as appropriate.

Recommendation b: Monitor the Joint Staff unified command supporting systems list to determine the status of its supporting systems and assess the impact to the U.S. Central Command area of responsibility mission and develop operational contingency plans accordingly.

USCENTCOM Comments: Concur. The Joint Staff is doing a good job of consolidating information from the unified commands and determining the status of those systems that affect multiple CINCs. Reviewing their documentation will help us determine if we are at risk and what contingency plans may be necessary.

Recommendation c: Complete the identification of mission-critical supporting systems that Services or other organizations manage and the owners of all of its supporting systems.

USCENTCOM Comments: Concur. Progress in identifying which of the systems in use within USCENTCOM and the owners of those systems is a regular part of our Year 2000 quarterly reports to the Joint Staff.

Recommendation d: Complete the identification of system interfaces and prepare written interface agreements for mission-critical systems that the U.S. Central Command manages.

USCENTCOM Comments: Concur. Progress in identifying systems interfaces is a regular part of our Year 2000 quarterly reports to the Joint Staff. We will update the reports to indicate whether or not an interface agreement exists.

Recommendation e: Develop contingency plans for U.S. Central Command managed mission-critical systems.

USCENTCOM Comments: Concur. U.S. Central Command is taking action to make our 17 systems Year 2000 compliant by the end of this year and have an additional year to clean up any systems we may have missed. We do not expect any Year 2000 related problems to cause catastrophic failures. We will prepare contingency plans for any system whose progress begins to slip.

Recommendation f: Review and assess contingency plans for mission-critical supporting systems and develop operational contingency plans as needed.

USCENTCOM Comments: Concur. Reviewing mission-critical supporting systems contingency plans will help us determine if we are at risk and what additional contingency plans may be necessary.

Recommendation g: Research Year 2000 compliance of vendor software and test mission-critical vendor software for Year 2000 compliance.

USCENTCOM Comments: Concur. We are researching the Year 2000 compliance status of COTS products used in USCENTCOM but only those products not tested by other federal agencies need to be considered for testing by USCENTCOM.

Recommendation h: Document test plans to show how managed systems were deemed compliant and determine the level of Year 2000 compliance.

USCENTCOM Comments: Concur. Although testing can not provide 100% assurance a problem will not occur, documenting the tests will allow us to know which scenarios have already been looked at, reducing future testing should problems occur.

Recommendation i: Coordinate Year 2000 solutions and contingency plans with U.S. Central Command component commands.

USCENTCOM Comments: Concur. USCENTCOM welcomes the sharing of information with its component commands.

Recommendation j: Use selected command and joint exercises to test Year 2000 scenarios in an operational environment.

USCENTCOM Comments: Concur. During exercises we use operational systems. Thus, turning the clocks ahead during exercises could impact real world operations. However, a carefully designed scenario, utilizing systems isolated from the operational environment, could be effectively and safely used to determine if critical systems are ready for the Year 2000.

Joint Staff Comments

THE JOINT STAFF
WASHINGTON, DC

Reply ZIP Code:
20318-0300

DJSM 663-98
19 June 1998

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

Subject: Audit Report on US Central Command Year 2000 Issues

1. The Joint Staff endorses your suggestions to improve the Year 2000 posture of the US Central Command (USCENTCOM).[1] We are fully committed to ensuring the warfighting missions of the combatant commands will be conducted without Year 2000-related mission degradation.

2. Your draft audit report included findings for both the Joint Staff and USCENTCOM. The Joint Staff's management comments on the draft audit are described in Enclosure A. USCENTCOM's management comments are shown at Enclosure B. *

3. The Joint Staff point of contact for Year 2000 actions is Lieutenant Colonel Ramona Barnes, J6V, (703) 695-2117, DSN 225-2117, ramona.barnes@js.pentagon.mil.

DC Blair
DENNIS C. BLAIR
Vice Admiral, U.S. Navy
Director, Joint Staff

Enclosures

Reference:
1 IG/DOD memorandum, 22 April 1998, "Audit Report on U.S. Central Command Year 2000 Issues (Project No. 8AS-0006.010"

*Enclosure B not included because CENTCOM submitted comments separately.

ENCLOSURE A

JOINT STAFF COMMENTS ON AUDIT REPORT ON US CENTRAL COMMAND YEAR 2000 ISSUES (PROJECT NO. 8AS-0006.01)

RECOMMENDATION 1: Develop and maintain a comprehensive inventory list of mission-critical supporting systems to enable the unified commands to monitor the progress of the Services and agencies and to assess the impact of mission operations.

JOINT STAFF COMMENTS: Concur. The Joint Staff Year 2000 Coordinator maintains a list of supporting systems identified by the combatant commands. The Department of Defense Year 2000 Project Office is developing a data base of all mission critical and non-mission critical systems in the Department. The Joint Staff and combatant commands will have access to this data base for researching Y2K status of supporting systems.

RECOMMENDATION 2. Assist the unified commands in obtaining year 2000 information on mission-critical supporting systems that Services or other organizations manage.

JOINT STAFF COMMENTS: We are working closely with the Services and Defense agencies to ensure mission critical supporting systems identified by the combatant commands are addressed as mission critical by the system owners. Additionally, the Joint Staff has functional proponents across the staff who are engaging on warfighting issues resulting from the Year 2000 challenge. Since the Office of the Secretary of Defense for Command, Control, Communications, and Intelligence (OSD/C3I) decided to terminate the use of the Defense Integrated Support Tools (DIST) data base for Year 2000 reporting, the Joint Staff is actively supporting the DOD Y2K Project Office initiative to create a new DOD Y2K mission critical systems data base to give the warfighters visibility into Year 2000 actions for all such systems supporting their respective missions.

RECOMMENDATION 3: Implement procedures to monitor and track the status of mission-critical supporting systems.

JOINT STAFF COMMENTS: Concur. The Joint Staff engages in significant coordination with the Services and Defense agencies on Y2K status of mission critical supporting systems. The Joint Staff's strong involvement in the development of a DOD-wide systems data base to catalog Y2K status and ongoing initiatives will further enhance the information flow.

RECOMMENDATION 4: Coordinate with the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to obtain and

Enclosure A

disseminate Year 2000 information on commercial off-the-shelf and Government off-the-shelf products.

JOINT STAFF COMMENTS: Concur. The Joint Staff is actively engaged in obtaining Y2K updates from commercial industry and government off-the-shelf product suppliers. This is an area of concern across the Federal government.

RECOMMENDATION 5: Assist the unified commands in testing systems and applications that are common to the unified commands.

JOINT STAFF COMMENTS: Concur. The Joint Staff has been facilitating the use of the Joint Interoperability Test Command (JITC) for Year 2000 testing of systems owned by the unified commands, as well as those owned by the Services and Defense agencies that support combatant command missions. Additionally, the Joint Staff engages the vendors that provide the many commercial-off-the-shelf products common to the combatant commands on Year 2000 issues.

RECOMMENDATION 6. Integrate Year 2000 scenarios into operational requirements in joint exercises starting in FY 1998 for the purposes of determining the extent of potential Year 2000 impact on continuity of warfighter operations.

JOINT STAFF COMMENTS: Concur. The Joint Staff is developing a Year 2000 Operational Evaluation Plan for use by the unified commands and the Services during exercises and other opportunities from now until Year 2000. Our goal is to ensure missions do not fail due to Y2K perturbations.

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report.

Thomas F. Gimble
Patricia A. Brannin
Mary Lu Ugone
Dianna J. Pearson
Scott S. Brittingham
Richard B. Vasquez
Jennifer L. Zucal
Maria R. Palladino