~~FOR OFFICIAL USE ONLY~~

Audit Report

JOINT CENTERS' YEAR 2000 ISSUES

Report No. 99-015 October 16, 1998

Office of the Inspector General
Department of Defense

~~FOR OFFICIAL USE ONLY~~

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

JBC	Joint Battle Center
JC2WC	Joint Command and Control Warfare Center
JCSE	Joint Communications Support Element
JWAC	Joint Warfare Analysis Center
JWFC	Joint Warfighting Center
Y2K	Year 2000

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

October 16, 1998

MEMORANDUM FOR COMMANDER IN CHIEF, U.S. ATLANTIC COMMAND
COMMANDER, JOINT WARFIGHTING CENTER
COMMANDER, JOINT COMMAND AND CONTROL WARFARE CENTER
COMMANDER, JOINT BATTLE CENTER
COMMANDER, JOINT WARFARE ANALYSIS CENTER
COMMANDER, JOINT COMMUNICATIONS SUPPORT ELEMENT

SUBJECT: Audit Report on the Joint Centers' Year 2000 Issues
(Report No. 99-015)

We are providing this report for review and comment. The Joint Command and Control Warfare Center did not respond to the draft report; however, we considered comments from the Joint Communication Support Element, Joint Warfare Analysis Center, and Joint Warfighting Center in preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Joint Communication Support Element, Joint Warfare Analysis Center, and Joint Warfighting Center comments were fully responsive. We request that the Joint Command and Control Warfare Center provide comments on all recommendations by November 16, 1998.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to [redacted] at (703) 604-[redacted] (DSN 664-[redacted]) <email [redacted]@dodig.osd.mil>, [redacted] at (703) 604-[redacted] (DSN 664-[redacted]) <email [redacted]@dodig.osd.mil>, or [redacted] at (703) 604-[redacted] (DSN 664-[redacted]) <email [redacted]@dodig.osd.mil>. See Appendix H 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. 99-015 **October 16, 1998**
(Project No. 8AS-0006.05)

Joint Centers' Year 2000 Issues

Executive Summary

Introduction. This 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 the issue, see the year 2000 webpage on the 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.

We reviewed the year 2000 programs for five Joint Centers that were transitioned from the Joint Staff to U.S. Atlantic Command effective October 1, 1998. The five Joint Centers are the Joint Battle Center, the Joint Command and Control Warfare Center, the Joint Communications Support Element, the Joint Warfare Analysis Center, and the Joint Warfighting Center. These centers carry out functions in the areas of joint training, joint doctrine and operational concept development, joint warfighting support and joint communications support.

Audit Objectives. The overall audit objective was to evaluate the status of the progress of the five Joint Centers 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, contingency planning, and support received from responsible Service executive agents.

Audit Results. The Joint Centers had taken several positive actions to address year 2000 computing issues; however, they had not fully addressed all potential year 2000 computing problems. Generally, the Joint Centers had not assessed all mission-critical systems for year 2000 compliance status, adequately certified and documented mission-critical systems as year 2000 compliant, developed contingency plans, and coordinated year 2000 efforts with the U.S. Atlantic Command and the Joint Staff. Consequently, there was continued risk that four of the five Joint Centers may be unable to fully execute their missions. Further, there was still risk that the Joint Centers may not be able to effectively facilitate or participate in year 2000 operational evaluations.

Summary of Recommendations. We recommend that the Commanders of four Joint Centers take immediate action to complete the assessment for determining the year 2000

compliance status of all mission-critical systems, certify and document all internally managed compliant systems, and develop contingency plans for all mission-critical systems that are not scheduled to be compliant by December 31, 1998.

Management Comments. The Joint Communication Support Element, Joint Warfare Analysis Center, and Joint Warfighting Center concurred with the recommendations. The Joint Command and Control Warfare Center did not comment on a draft of this report that was issued August 21, 1998. We request that the Commander, Joint Command and Control Warfare Center, provide comments to the final report by November 16, 1998. See Part I for a summary of management comments and Part III for the complete text of the comments.

Table of Contents

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 system and application programs that use dates to calculate, compare, or sort could generate incorrect results when working with years following 1999. Calculating 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 Year 2000 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) Version 1.0 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. The DoD Management Plan, for Signature Draft Version 2.0, June 1998, accelerates the target completion dates for the renovation, validation, and implementation phases. The new target completion date for implementation of mission critical systems is December 31, 1998.

Office of the Secretary of Defense Memorandums. The Secretary of Defense and the Deputy Secretary of Defense have issued recent memorandums on DoD Y2K efforts.

Year 2000 Compliance. On August 7, 1998, the Secretary of Defense issued the memorandum, "Year 2000 Compliance," stating that the DoD is making insufficient progress in its efforts to solve its Y2K problem. The

memorandum requires the Chairman of the Joint Chiefs of Staff to develop a joint Y2K operational evaluation program to be completed by October 1, 1998. Further, effective October 1, 1998, the memorandum designates responsibility to the Services, unified commands, and Defense agencies for ensuring that:

- The list of mission-critical systems is accurately reported in the DoD Y2K database.
- Funds are not obligated for any mission-critical system in the Y2K database that lacks a complete set of formal interface agreements for Y2K compliance.
- Funds are not obligated for any information technology or national security system contract that processes date-related information and that does not contain the Y2K requirements specified in Section 39.106 of the Federal Acquisition Regulation.
- Funds are not obligated for any domain user in a Defense Information Systems Agency megacenter if that domain user has failed to sign all associated explicit test agreements.

Year 2000 Verification of National Security Capabilities. On August 24, 1998, the Deputy Secretary of Defense issued the memorandum, "Year 2000 Verification of National Security Capabilities." The memorandum requires DoD Components to verify that all functions will continue unaffected by Y2K issues and to certify that they have tested the information technology and national security systems in accordance with the DoD Y2K Management Plan. The DoD Components are required to submit testing plans and certifications to the Deputy Secretary of Defense by November 1, 1998.

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

Realignment of Joint Centers U.S. Atlantic Command. In an effort to reduce any parallel functions that exist between the Joint Staff and the Office of the Secretary of Defense, five Joint Centers are being realigned under U.S. Atlantic Command. The five Joint Centers are the Joint Battle Center (JBC), the Joint Command and Control Warfare Center (JC2WC), the Joint Communications Support Element (JCSE), the Joint Warfare Analysis Center (JWAC), and the Joint Warfighting Center (JWFC). According to the Defense Reform Initiative, it was appropriate for the Joint Centers to report to a tactical unified command rather than to the Joint Staff because the Joint Centers were providing support at the tactical, operational, and strategic levels.

Joint Battle Center, Suffolk, Virginia. The JBC provides the unified commands with a joint command, control, communications, computers, intelligence, surveillance, and reconnaissance assessment, and experimentation capability.

Joint Command and Control Warfare Center, Kelly Air Force Base, Texas. The JC2WC provides the Joint Staff and unified commands with the expertise in planning and executing command and control warfare and information operations.

Joint Communications Support Element, Tampa, Florida. The JCSE provides contingency and crisis communications to meet the operational and support needs of the unified commands, Services, Defense agencies and Non-Defense agencies.

Joint Warfare Analysis Center, Dahlgren, Virginia. The JWAC provides the Joint Staff and unified commands with effects-based, precision targeting options necessary for selected networks and nodes to carry out the national security and military strategies during peace, crisis, and war.

Joint Warfighting Center, Fort Monroe, Virginia. The JWFC assists the Joint Staff, unified commands and Service Chiefs of Staff in preparing joint and multi-national operations, through the conceptualization, development, and assessment of current and future joint doctrine, and accomplishing joint and multi-national training and exercises.

Audit Objectives

The overall audit objective was to evaluate the status of progress of the five Joint Centers in resolving the 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, contingency planning, and support received from responsible Service executive agents. See Appendix A for a discussion of the audit scope and methodology and for a summary of prior coverage.

Status of the Joint Centers' Year 2000 Program

The Joint Centers had taken several positive actions to address Y2K computing issues; however, they had not fully addressed all potential Y2K problems. Generally, the Joint Centers had not fully:

- assessed all mission-critical systems for Y2K compliance status;
- certified and documented mission-critical systems as Y2K compliant;
- developed contingency plans; and
- coordinated Y2K efforts with the Joint Staff.

Consequently, there was continued risk that four of the five Joint Centers may be unable to fully execute their missions. Further, there was still risk that the Joint Centers may not be able to effectively facilitate or participate in Y2K operational evaluations.

Positive Actions

The Joint Centers have recognized the importance of the Y2K computing problem and have taken several positive actions to address Y2K issues. Specifically, the Joint Centers developed a Y2K strategic plan, established a Y2K team with focal points throughout each command, required that all acquisitions be Y2K compliant, and identified mission-critical systems. See Appendixes C through G for the complete results of each Joint Center site visit[1].

Y2K Strategic Plan. The Joint Centers developed Y2K plans that are consistent with the DoD Y2K Management Plan and the Joint Staff Y2K Action Plan. The Joint Center Y2K plans provide an overall strategy and include specific steps necessary to address the Y2K problem. For example, the JCSE Y2K Plan provides an overall management strategy and implements the DoD compliance phase process by listing the steps necessary to complete each phase.

Y2K Teams. The Joint Centers established Y2K teams with functional area managers to fully coordinate Y2K efforts within the commands. The Y2K teams meet periodically to discuss system mission criticality, progress, and areas of concern.

[1]The results of the site visits were documented in point papers and were briefed to each Joint Center Commander or representative before leaving the site. However, the point papers have been revised to reflect current information.

Acquisitions of Information Technology. The Joint Centers require that all acquisitions of information technology be Y2K compliant. The Joint Centers included the appropriate Federal Acquisition Regulation statements in contracts and have taken appropriate action to address the issue. For example, JWAC and JWFC have an acquisition process that ensures all purchases of software, hardware, and renewal of software licenses are Y2K compliant.

Joint Warfare Analysis Center. Beginning in December 1997, JWAC implemented controls that required all information technology procurement packages exceeding $100,000 to comply with Federal Acquisition Regulation 39.106[2]. Further, JWAC has a Production Change Control Board, primarily consisting of members of the JWAC Y2K team, which is responsible for approving all acquisitions of information technology. The Control Board is required to obtain statements from vendors stating that the technology purchased is Y2K compliant.

Joint Warfighting Center. The JWFC requires that all acquisitions of automated data processing equipment are approved by the Y2K project manager, who verifies with the vendor that the equipment being purchased is Y2K compliant. The Y2K project manager approves acquisitions only after adequate documentation is obtained to support Y2K-compliant status.

Identifying Mission-Critical Systems. The Joint Centers have taken appropriate action to identify mission-critical systems. They have developed a mission-critical systems inventory, which includes internally developed mission-critical systems and also systems that are managed by other Government and DoD agencies. A mission-critical systems list is the starting point for assessment and prioritization.

Joint Exercises/Operational Evaluations

Two of the Joint Centers may be able to provide assistance to the DoD Y2K effort by including Y2K simulations as part of joint exercises. The Joint Centers consist of multi-Service representatives who participate in joint exercises to perform real time Y2K validation and interface testing. Specifically, JBC and JWFC stated that they may be able to include Y2K scenarios as part of joint exercises.

Joint Battle Center. The JBC conducts assessments of newly developed systems to determine utility to the warfighter. The JBC is using the assessment process to provide Y2K validation by incorporating Y2K into the assessment process. During an assessment, JBC will determine the Y2K compliance status of the systems under review and potential Y2K issues. Any potential Y2K effects will be documented in either an interim report or in the final assessment report. Additionally, JBC will validate systems that are claimed to be Y2K compliant during assessments. Further, JBC is determining how Y2K simulations can be

[2] Federal Acquisition Regulation 39.106 specifies that all information technology acquisitions be Y2K compliant.

included in the joint operational exercise phase of assessments. If feasible, JBC may include a Y2K simulation as part of the joint operational exercise phase of the assessment.

Joint Warfighting Center. The JWFC is determining whether its training and exercise division should include Y2K scenarios in its various joint exercises. The JWFC has stated that it will make that determination when the exercise division returns from its current deployment.

Assessment of Mission-Critical Systems

The Joint Centers have not fully assessed all mission-critical systems for Y2K compliance. As of July 1998, the Joint Centers had not assessed 56 of 100 mission-critical systems for compliance; therefore, their compliance status is unknown and awaiting determination. As part of the assessment phase, the DoD Y2K Management Plan requires that all mission-critical systems be analyzed for Y2K compliance. The Joint Centers need to fully determine the Y2K compliance status for all mission-critical systems to ensure that the warfighting mission will not be adversely affected. The following table shows the Y2K compliance status for the Joint Centers' maintained and supporting mission-critical systems as of August 1998. See Appendix B for a summary of the status of the Joint Centers' Y2K Program and Appendixes C through G for complete details of each site visit.

Compliance Status for the Joint Centers' Mission-Critical Systems[3]

	Compliant	Noncompliant	Unknown	Total
JBC	0	0	0	0
JC2WC	9	6	21	36
JCSE	9	6	13	28
JWAC	2	3	12	17
JWFC	5	4	10	19
Total	**25**	**19**	**56**	**100**

The JBC stated that it did not identify any mission-critical systems because the equipment used to perform assessments varies by project. The JBC generally uses equipment and systems that are brought in specifically to conduct each individual assessment.

[3] Includes internally managed systems and supporting systems that are managed by other Government and DoD agencies. Does not include systems that are scheduled to be retired or replaced before December 31, 1999.

Compliance Certification and Documentation

The Joint Centers have not adequately certified and documented mission-critical systems that are Y2K compliant. The previous table shows 100 Joint Center mission-critical systems, of which 41 are internally managed and 59 are managed by other Government and DoD agencies. Of the 41 internally managed systems, 11 have been identified by the Joint Centers as Y2K compliant. The Joint Centers maintained compliance checklists for some of the 11 compliant systems, but they were incomplete, unsigned, or both. Inadequate certification and documentation is a major area of concern and a DoD-wide problem. The Inspector General Report No. 98-147, "Year 2000 Certification of Mission-Critical DoD Information Technology Systems," states that DoD Components are not complying with Y2K certification criteria before reporting systems as compliant. The Report states that of the 430 systems that DoD reported as Y2K compliant, only 109 were certified. Mission-critical systems may unexpectedly fail because they were identified as compliant without being validated. The Joint Centers need to ensure that compliant systems are validated and that adequate documentation exists to support the compliant status.

Contingency Plans

Contingency plans provide for continuity of core processes regardless of any system failure caused by the Y2K; however, the Joint Centers have not developed contingency plans for mission-critical systems. According to the Joint Staff Y2K Action Plan, all mission-critical systems that are not Y2K compliant and fully implemented by December 31, 1998, must have a contingency plan. The Joint Centers will not have all mission-critical systems compliant by December 31, 1998, and therefore should develop contingency plans for all mission-critical systems that are behind schedule.

Coordinating Y2K Efforts

The Joint Centers had not fully coordinated Y2K efforts with the Joint Staff. As of May 1998, the Joint Centers had not reported the status of their mission-critical systems to the Joint Staff. Because the Joint Staff reports Y2K efforts to DoD for all the unified commands, it should be fully aware of the Joint Centers' Y2K status. As of July 1998, the Joint Centers and U.S. Atlantic Command had begun to take action to coordinate the status of their Y2K programs, prior to the official October 1, 1998, transition date. We consider the actions of the Joint Centers and U.S. Atlantic Command to be commendable.

Conclusion

Although they have made some progress to resolve potential Y2K problems, four of the five Joint Centers face a high risk that Y2K-related disruptions will impair mission capabilities. The JBC has a commendable Y2K program in place, while the other four centers need to take immediate action to comply with Joint Staff and DoD guidance. DoD has established December 31, 1998, for all mission-critical systems to be fully compliant, tested and implemented. With less than 3 months remaining, the Joint Centers must take a more aggressive approach to resolve potential Y2K computing problems. Unless further progress is made, the Joint Centers' ability to facilitate or participate in Joint Service warfighting exercises may be impacted.

Recommendations and Management Comments

We recommend that the Commander, Joint Communications Support Element; Commander, Joint Command and Control Warfare Center; Commander, Joint Warfare Analysis Center; and Commander, Joint Warfighting Center take immediate action to:

1. **Complete the assessment for determining the year 2000 compliance status of all mission-critical systems.**

2. **Certify and document all internally managed compliant systems.**

3. **Develop contingency plans for all mission-critical systems that are not scheduled to be compliant by December 31, 1998.**

Management Comments. The Commander, Joint Communications Support Element; Commander, Joint Warfare Analysis Center; and Commander Joint Warfighting Center concurred with all of the recommendations and described the progress made and completion dates for each recommendation.

Management Comments Required. The Joint Command and Control Warfare Center did not comment on the draft report. We request that the Joint Command and Control Warfare Center provide comments on the final report by November 16, 1998.

Part II - Additional Information

Appendix A. Audit Process

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

Scope

We reviewed and evaluated the Joint Centers' Y2K programs in accordance with DoD, Joint Staff and U.S. Atlantic Command guidance. We visited each Joint Center to determine the status of its Y2K program. The results of each site visit are detailed in Appendixes C through G. Each Joint Center Commander was briefed upon departing the site. At each Joint Center, we evaluated the Y2K programs in the following areas: systems inventory, assessment, acquisitions of information technology, cost estimates, contingency plans, and coordination of efforts with Joint Staff and U.S. Atlantic Command. We interviewed members of the Joint Center Y2K teams to determine the level of involvement at the various management levels. We obtained and analyzed documentation that the Joint Centers used to determine the compliance status for mission-critical systems.

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 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 May through July 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.

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. Summary of the Joint Centers' Year 2000 Program

	JBC	JC2WC[1]	JCSE	JWAC[1]	JWFC
Y2K program phase[2]	3	2	2	2	2
Y2K plan	Yes	Draft	Yes	Yes	Yes
Y2K team	Yes	Yes	Yes	Yes	Yes
MC[3] maintained systems	0	5	13	6	17
Compliant[4]	0	5	0	1	5
Noncompliant	0	0	2	0	3
Status unknown	0	0	11	5	9
MC[3] supporting systems	0	31	15	11	2
Compliant	0	4	9	1	0
Noncompliant	0	6	4	3	1
Status unknown	0	21	2	7	1
Contingency plans	N/A[5]	None	None	None	None
Acquisitions required to be Y2K compliant	Yes	Yes	Yes	Yes	Yes
Risk of Y2K problems[6]	Low	High	High	High	High

[1] Some intelligence systems are not included in the totals because of their classification level.

[2] The five phase Y2K process consists of: 1) awareness, 2) assessment, 3) renovation, 4) validation, 5) implementation.

[3] MC is mission critical. Mission-critical maintained systems are internally developed by the respective Joint Center. Mission-critical supporting systems are maintained by other Government or DoD agencies.

[4] Although the numbers shown represent compliant systems as identified by the Joint Centers, the compliance checklists used to support compliance status were incomplete, unsigned, or both.

[5] JBC stated that because it has not identified any mission-critical systems, no contingency plans are needed.

[6] The risk is based on the following three factors: 1) number of mission-critical systems, 2) assessment of mission-critical systems, 3) number of mission-critical systems that have been identified as compliant.

Appendix C. The Joint Battle Center Year 2000 Program

The JBC Y2K effort is currently in the renovation phase and is in compliance with the Joint Staff Y2K Action Plan. The JBC has taken appropriate action to address the Y2K problem and has:

- established a Y2K team with focal points throughout the command;
- developed a Y2K Plan that includes a management strategy and key tasks with target dates;
- developed a complete systems inventory list;
- determined the Y2K-compliance status for all systems, software and hardware;
- obtained Y2K-compliance checklists for systems used in projects; and
- incorporated Y2K issues in its assessment procedures manual.

Systems Inventory

The JBC identified a total of 233 communications systems, video systems, infrastructure devices, hardware devices, and software that it uses in day-to-day operations. The JBC determined that 225 of the 233 systems are Y2K compliant and established a completion date of December 1998 to renovate the remaining 8 noncompliant systems. Further, the JBC has obtained sufficient documentation supporting the Y2K-compliance status for the 225 compliant systems.

Mission-Critical Systems

The JBC determined that it does not have any systems considered critical to its mission. The primary mission of JBC is to perform assessments on command, control, communications, computers, intelligence, surveillance and reconnaissance systems and determine utility to the Warfighter. When it performs assessments, JBC provides technical support and facilities to be used by the Warfighter, but special equipment and systems are brought in to JBC to conduct the assessment.

JBC Utility to DoD Y2K Effort

The JBC has incorporated Y2K language in its assessment procedures manual to include determining the Y2K-compliance status of the systems under review and any potential impact. Potential Y2K effects will be documented in either an interim report or in the final assessment report. Additionally, JBC will validate systems that are claimed to be Y2K compliant during assessments.

The JBC is determining how Y2K can be included in the joint operational exercise phase of assessments. The operational exercises provide an opportunity to validate Y2K system interfaces in a real-world environment. If feasible, the JBC may include a Y2K simulation as part of the joint operational exercise phase of the assessment.

JBC Transition to U.S. Atlantic Command

The JBC has coordinated its Y2K effort with the U.S. Atlantic Command and will begin reporting its Y2K status to the U.S. Atlantic Command beginning in July 1998, before the official October 1, 1998, realignment.

Appendix D. The Joint Communications Support Element Year 2000 Program

Status of Y2K Program

The JCSE Y2K effort is currently in the assessment phase and has implemented an aggressive schedule to comply with the Joint Staff Y2K plan by October 30, 1998. To date, JCSE has:

- established a Y2K team with focal points throughout the command;
- reinforced the importance of Y2K efforts at top levels of management;
- developed a Y2K plan that includes a management strategy and key tasks with target dates;
- developed a Y2K intranet web page to promote sharing information;
- developed inventory lists for each functional directorate, line company, and Air National Guard Unit;
- identified JCSE mission-critical systems;
- identified the executive agent and program manager for mission-critical systems; and
- obtained the Y2K compliance status for 15 of its 28 mission-critical systems.

Systems Inventory

The JCSE functional directorates and line companies have compiled inventory lists but may not have fully identified all systems. For example, a functional directorate identified all computers and equipment but did not identify a system that operated on the equipment.

Suggested Action. Establish guidance on requirements of a reportable system.

Mission-Critical Systems

Systems critical to the JCSE mission may not be listed on the Services' and agencies' mission-critical systems lists. The JCSE has identified 28 mission-critical systems, of which 15 are managed by the Services and other Defense organizations. As of May 1998, the JCSE identified executive agents for the 28 JCSE mission-critical systems as follows.[4]

7	Army	0	Navy
13	JCSE	4	Air Force
3	DISA*	1	SOCOM*

*DISA is the Defense Information Systems Agency and SOCOM is the U.S. Special Operations Command.

We reviewed the March 1998 Army mission-critical systems list and compared it to the JCSE mission-critical list. None of the seven Army managed systems was listed on the Army mission-critical list.

Suggested Action. The JCSE, with the help of the Joint Staff and U.S. Atlantic Command, needs to provide a list of mission-critical systems to the appropriate executive agents, and recommend that they add systems to their mission-critical systems lists.

JCSE Transition to U.S. Atlantic Command

The JCSE needs to coordinate with the U.S. Atlantic Command, the other four Joint Centers that are transitioning to the U.S. Atlantic Command, and the Joint Staff on its Y2K effort. The five Joint Centers should be incorporated into the U.S. Atlantic Command Y2K program in the same manner.

[4] JCSE provided updated information on August 6, 1998, which was included in the report. The numbers shown here reflect the status as of May 1998.

Appendix E. The Joint Command and Control Warfare Center Year 2000 Program

Status of Y2K Program

The JC2WC has taken several positive actions to address the Y2K problem. To date, JC2WC has:

- established a Y2K team with focal points throughout the command,
- developed a draft Y2K Compliance Plan,
- developed a systems, software and hardware inventory, and
- coordinated Y2K efforts with the Air Force Intelligence Agency.

The JC2WC Y2K effort is in the assessment phase. According to the DoD Y2K Management Plan, JC2WC needs to complete the following steps to move into the renovation phase:

1. Develop contingency plans for mission-critical systems that will not be compliant by December 31, 1998.
2. Complete the analysis to determine the Y2K compliance status for all systems, software and hardware.
3. Prioritize systems requiring renovation.

Systems Inventory

The JC2WC developed a systems inventory and took appropriate action to identify systems, software and hardware. The JC2WC systems inventory consists of internally developed analysis, planning, and training simulation models, systems managed by other Government and DoD agencies, and commercial-off-the-shelf software and hardware. The JC2WC systems inventory consists of 8 maintained systems, 31 systems managed by other Government agencies, and 492 software and hardware components. The systems inventory includes relevant information such as the Y2K compliance status, system POC, and functional area.

Y2K Compliance Status

The JC2WC has obtained the Y2K compliance status for some of its systems and software and hardware. Of the 31 systems that are maintained by other Government and DoD agencies, 4 have been identified as Y2K compliant, 21 as

unknown or blank, and 6 as noncompliant. Of the 492 software and hardware components, 212 have been identified as Y2K compliant, 272 as unknown and 8 as noncompliant. The JC2WC needs to complete the analysis to determine the status of systems, software and hardware.

Suggested Action. Complete the assessment for determining the Y2K compliance status of all mission-critical systems.

Mission-Critical Systems

The JC2WC has five mission-critical systems to renovate and validate for Y2K compliance. The JC2WC systems inventory identifies the five systems as Y2K compliant, but still in the validation phase. The JC2WC is completing Y2K compliance checklists for its five mission-critical systems and will internally test and self-certify the systems for Y2K compliance.

Contingency Plans

The JC2WC has not developed contingency plans for its five maintained systems in the validation phase. The JC2WC stated that the maintained systems are scheduled to be compliant before December 31, 1999. However, the Joint Staff Y2K Action Plan requires contingency plans to be developed for mission-critical systems that will not be compliant by December 31, 1998. The JC2WC Y2K plan and the systems inventory list do not indicate completion dates for its maintained systems; therefore, JC2WC needs to determine the completion date for renovating its mission-critical systems and prepare contingency plans for those systems that will not be Y2K compliant by December 31, 1998.

Suggested Action. Develop contingency plans for those systems that will not be Y2K compliant and fully implemented by December 31, 1998.

JC2WC Transition to U.S. Atlantic Command

The JC2WC has reported the status of its Y2K efforts to the Air Force Intelligence Agency using Air Force guidance and direction, JC2WC has not reported its Y2K status to the Joint Staff or the Unified Commands. The Joint Staff and U.S. Atlantic Command need to be aware of the JC2WC mission-critical systems and their Y2K-compliance status to fully coordinate the Joint Staff Y2K effort.

Suggested Action. The JC2WC should immediately begin reporting the status of its Y2K efforts to U.S. Atlantic Command. At a minimum, JC2WC should report the total number of mission-critical systems, the number of mission-critical

systems in each phase outlined in the Joint Staff Y2K Action Plan, and the number of systems that will not be Y2K compliant and fully implemented by December 31, 1998.

In addition, adequate funding may not be available to JC2WC to address all Y2K issues because the JC2WC Y2K Plan states that adequate funding may not be available to correct Y2K problems. The JC2WC plan also states that some JC2WC server platforms may cost more than $20,000 each and individual personal computers will cost more than $2,000 per desktop. The Joint Staff and the U.S. Atlantic Command need to be aware of funding issues to ensure that the JC2WC mission will not be affected by Y2K.

Suggested Action. Immediately report funding issues and other areas of concern to the U.S. Atlantic Command and the Joint Staff.

Appendix F. The Joint Warfare Analysis Center Year 2000 Program

Status of Y2K Program

The JWAC has taken several positive actions to address the Y2K problem. To date, JWAC has:

- established a Y2K team with focal points throughout the command;
- developed a Y2K Plan that includes a management strategy and key tasks with target dates;
- developed a systems inventory
- identified mission-critical systems and software and hardware; and
- obtained Y2K-compliance status for most of its systems and software and hardware;

The JWAC Y2K effort is near the end of the assessment phase. According to the DoD Y2K Management Plan, JWAC needs to complete the following steps to move into the renovation phase:

1. Develop contingency plans for mission-critical systems.
2. Complete the analysis to determine the Y2K-compliance status for all systems and software and hardware.

Systems Inventory

The JWAC has a complex inventory consisting of systems with multiple platforms that include many software, hardware, and models and simulation packages. JWAC has taken appropriate action to identify all systems and software and hardware that are in its systems inventory. The JWAC systems inventory has 19 systems that are managed by JWAC, 16 systems that are maintained by other Government agencies, and 188 software and hardware components. The systems inventory includes key system information such as the name, mission criticality, and Y2K compliance status; however, it is missing information that is necessary to determine the Y2K compliance status for systems that are owned and maintained by other Government and DoD agencies.

Suggested Action. Obtain the following information and include it in each system inventory that is managed by other Government and DoD agencies:

- the executive agent responsible for maintaining the system, and
- the program manager or point of contact for the system.

This information will help to determine the Y2K-compliance status and update the status as each system moves toward Y2K compliance.

Y2K Compliance Status

The JWAC has obtained the Y2K-compliance status for a majority of its systems and software and hardware. Of the 19 systems that JWAC maintains, 12 are Y2K compliant, 6 are pending determination and 1 does not have any date or time Y2K implications. Of the 16 systems maintained by other Government and DoD agencies, 2 are "yes", 3 as "no", 6 as "yes/no", and 5 as "tbd" (to be determined) for Y2K compliance status. The JWAC needs to clarify the Y2K-compliance status for each system by indicating the appropriate phase that each system is in, instead of yes, no, yes/no and tbd. According to the Joint Staff Y2K Plan, the appropriate phases for a system as it moves toward Y2K-compliance status are awareness, assessment, renovation, validation, implementation, replacement, retirement or completed[5].

Suggested Action. Determine the appropriate Y2K-compliance phase for all systems.

Testing and Validating Mission-Critical Systems

JWAC has six mission-critical systems to renovate and validate for Y2K compliance and only one has been identified as Y2K compliant because JWAC did not provide adequate documentation to support the Y2K-compliance status. In addition, JWAC uses 42 mission-critical commercial-off-the-shelf products, and only 21 were Y2K compliant. Although JWAC obtained vendor compliance statements and other information to support the compliance status, it should perform validation and testing to ensure that Y2K-related disruptions will not impair mission capabilities. The JWAC stated that is planning to validate and test mission-critical systems and commercial-off-the-shelf products later this year.

Suggested Action. During the validation phase, test mission-critical systems and commercial-off-the-shelf products for Y2K compliance and document the results in the Y2K compliance checklists as specified in the DoD Y2K Management Plan.

[5] This differs from the DoD five-phase process because the Joint Staff database requires the additional phases; replacement, retirement and completed for reporting and tracking purposes.

Written Interface Agreements

The JWAC identified external source data feeds critical to the JWAC mission. The JWAC list of external interfaces includes appropriate and relevant information such as the type of data, source, media feed, frequency, clearance classification, and date format. The external interfaces include data feeds from Defense intelligence agencies and various contractors. JWAC is confident that all Y2K issues concerning external interfaces will be resolved; however, to ensure that external interfaces are Y2K compliant, JWAC should obtain written interface agreements with each data feed source.

Suggested Action. Obtain written interface agreements for all external source data feeds.

Contingency Plans

The JWAC has not developed contingency plans for the six JWAC-managed systems. The JWAC Y2K plan states that all systems should be Y2K compliant before the year 2000 and, if systems will not be compliant, a contingency plan should be developed according to the Joint Staff Y2K Action Plan guidelines. However, the Joint Staff Y2K Action Plan states that any mission-critical system that is not Y2K compliant and fully implemented by December 31, 1998, must have a contingency plan.

Suggested Action. Develop contingency plans for those systems that will not be Y2K compliant and fully implemented by December 31, 1998.

Acquisitions

The JWAC has an acquisition process that ensures all purchases of software, hardware, and software license renewals are Y2K compliant. In December 1997, JWAC implemented controls requiring all information technology procurement packages exceeding $100,000 to comply with Federal Acquisition Regulation 39.106[6]. Further, JWAC has a Production Change Control Board (the Board), which primarily consists of members of the JWAC Y2K team that approves all acquisitions of information technology. The Board is required to obtain documentation from vendors stating that the technology purchased is Y2K compliant. The JWAC has taken appropriate action to address this issue.

[6] Federal Acquisition Regulation 39.106 specifies that all information technology acquisitions be Y2K compliant.

JWAC Transition to U.S. Atlantic Command

The JWAC reported the status of its Y2K efforts to its Executive Service, but did not report its Y2K status to the Joint Staff or the unified commands. The Joint Staff and the U.S. Atlantic Command need to be aware of JWAC mission-critical systems and their Y2K compliance status to fully coordinate the Joint Staff Y2K effort.

Suggested Action. The JWAC should immediately begin reporting the status of its Y2K efforts to the U.S. Atlantic Command. At a minimum, JWAC should report the total number of mission-critical systems, the number of mission-critical systems in each phase outlined in the Joint Staff Y2K Action Plan, and the number of systems that will not be Y2K compliant and fully implemented by December 31, 1998.

Appendix G. The Joint Warfighting Center Year 2000 Program

Status of Y2K Program

The JWFC has taken several positive actions to address the Y2K problem. To date, JWFC has:

- established a Y2K team with focal points throughout the command,
- developed a Y2K plan that includes a management strategy and key tasks with target dates,
- reinforced the importance of Y2K issues at top levels of management,
- assessed 10 of 26 systems for compliance,
- developed a mission-critical systems inventory list; and
- required that all information technology acquisitions be Y2K compliant.

The JWFC Y2K effort is currently in the assessment phase. According to the DoD, Joint Staff, and Y2K Management Plans, JWFC needs to complete the following steps to move into the renovation phase:

1. Complete the assessment of all systems, and software and hardware to determine Y2K compliance status.
2. Develop contingency plans for all mission-critical systems that will not be fully compliant and implemented by December 31, 1998.

Systems Inventory

The JWFC operates an extensive mixed inventory of automation hardware and software systems that are or have the potential to be impacted by Y2K. The JWFC developed a systems inventory and has taken appropriate action to identify all systems, software and hardware. The system inventory includes key information such as the system name, JWFC proponent (the divisions that mainly use the system), and the system proponent (executive agent). The JWFC systems inventory consists of 19 mission-critical systems, of which 11 are managed by JWFC, 2 are managed by other Government and DoD agencies, and 6 are pending determination of the executive agent for the system. JWFC needs to identify the executive agent for all of its systems.

Suggested Action. Determine the executive agent for all systems.

Y2K Compliance Status – Mission-Critical Systems

The JWFC identified 19 mission-critical systems and determined the Y2K compliance status for some. Of 19 mission-critical systems, 9 have been assessed for Y2K compliance status. The following table shows the assessment progress for all JWFC mission-critical systems.

	Compliant	Noncompliant	Unknown	Total
JWFC Systems	5	3	9	17
Supporting Systems	0	1	1	2
Total	5	4	10	19

However, the JWFC has not determined the appropriate phase for all noncompliant systems. According to the Joint Staff Y2K Action Plan, the appropriate phases include awareness, assessment, renovation, validation, implementation, completed, retirement, or replacement. Indicating the phase will help to determine progress as each noncompliant system moves through the process. For example, the Joint Electronic Library is listed as noncompliant, but no phase is given. After interviewing personnel in the Doctrines Division, we found that the system had been assessed and was awaiting renovation. Specifically, the Solaris operating system for Joint Electronic Library was not compliant, but will be compliant when it is upgraded to version 2.6 or a later version. Therefore, the Joint Electronic Library should be listed appropriately in the renovation phase. The JWFC needs to determine the compliance status and the appropriate phase for all systems.

Suggested Action. Determine the Y2K compliance status and appropriate phase for all systems.

Testing and Validating Mission-Critical Systems

To date, JWFC has identified five mission-critical systems that are compliant. Although JWFC obtained vendor compliance statements and other information to support the compliance status for some of its system components, testing needs to be performed to ensure that Y2K-related disruptions will not impair mission capabilities

Suggested Action. During the validation phase, test mission-critical systems and document the results in the Y2K compliance checklists as specified in the DoD Y2K Management Plan.

Contingency Plans

The JWFC has not developed contingency plans for its mission-critical systems, although the Joint Staff Y2K Action Plan states that all mission-critical systems that are not Y2K compliant and fully implemented by December 31, 1998, must have a contingency plan.

Suggested Action. Develop contingency plans for those systems that will not be Y2K compliant and fully implemented by December 31, 1998.

Acquisitions

The JWFC has an acquisition process to ensure that all new purchases of information technology are Y2K compliant. All JWFC acquisitions exceeding $2,500 are "piggybacked" onto existing Service or other agency contracts. Our review showed that these contracts comply with Federal Acquisition Regulation 39.106[7]. In addition, all information technology acquisitions are required to be approved by the JWFC Y2K program manger. JWFC has taken appropriate action to address this issue.

JWFC Transition to U.S. Atlantic Command

The JWFC has not reported the status of its Y2K efforts to the Joint Staff, the U.S. Atlantic Command or other unified commands. However, JWFC reported that it has no funding issues for Y2K fixes to the Joint Staff. The Joint Staff and the U.S. Atlantic Command need to be aware of the JWFC mission-critical systems and their Y2K compliance status to fully coordinate the Joint Staff Y2K effort.

Suggested Action. Report the Y2K status to the U.S. Atlantic Command. At a minimum, JWFC should report all mission-critical systems, the appropriate phase of each system, and all systems that are not scheduled to be Y2K compliant and fully implemented by December 31, 1998.

[7] Federal Acquisition Regulation 39.106 specifies that all information technology acquisitions be Y2K compliant.

Conclusion

Because of its high reliance on automated systems, JWFC could lower the risk of Y2K problems by completing the assessment of all systems. Its highest Y2K priority should be to complete the assessment of all mission-critical systems. After the assessment is completed, JWFC will be able to fully estimate Y2K costs, renovate noncompliant systems, and develop contingency plans as needed.

Appendix H. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisitions and Technology
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Year 2000 Oversight and Contingency Planning Office
Assistant Secretary of Defense (Public Affairs)
Director, Operational Test and Evaluation

Joint Staff

Director, Joint Staff
Commander, Joint Battle Center
Commander, Joint Command and Control Warfare Center
Commander, Joint Communications Support Element
Commander, Joint Warfare Analysis Center
Commander, Joint Warfighting Center

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 Command
Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
    Inspector General, Defense Information Systems Agency
    Chief Information Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, Nation 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, Nation 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

Appendix H. Report Distribution

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

Joint Communications Support Element Comments

JOINT COMMUNICATIONS SUPPORT ELEMENT
8532 MARINA BAY DRIVE
MACDILL AIR FORCE BASE, FLORIDA 33621-5504

JCSE-J5A 21 Sep 98

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT DIRECTORATE
INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Management Comments to Audit Report on the Joint Centers' Year 2000 Issues

1. This is in response to the proposed audit report "Joint Centers' Year 2000 Issues". The report requested comments to applicable findings and recommendations. The overall audit objective was to evaluate the status of progress of JCSE in resolving the Y2K computing issue.

2. JCSE concurs with the recommendations made by the IG audit team. JCSE has taken the following actions as recommended:

a. JCSE has obtained the Y2K status on all 15-mission critical service/agency managed systems. We have established a point of contact for each system and JCSE is actively tracking the Y2K status. JCSE is currently preparing an official message addressed to each service and agency program manager requesting Y2K certification documentation. Estimated completion date: 2 Oct 98.

b. JCSE is currently developing a plan to perform an in-house Y2K operational evaluation. Due to heavy operational tasking, we have tentatively scheduled this evaluation for 8-12 March 1999. This evaluation will assess the Y2K status of the 13 JCSE owned mission critical systems. Estimated completion date: 12 Mar 99.

c. The JCSE Y2K representatives and J3 operational representatives have meetings scheduled to discuss the development of Y2K contingency plans. JCSE will develop operational contingency plans by 31 December 1998 for the JCSE owned systems. Estimated completion date: 31 Dec 98.

3. If you have any questions, please call my Y2K POC, (b) (6) at DSN 968 (b) (6)
(b) (6)

Joint Warfare Analysis Center Comments

Joint Warfare Analysis Center
Dahlgren, VA 22448-5500

IN REPLY REFER TO
5000
Ser J6/270
21 Sep 98

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

Subject: Draft of a Proposed Audit Report, Joint Centers' Year 2000 Issues (Project No. 8AS-0006.05)

1. This is in response to your request to review and comment on your 21 August audit report, subject as above. We concur with your recommendations with comments.

2. We request that you incorporate this memorandum along with the enclosed in the final audit report.

3. My point of contact is (b) (6) . (b) (6) can be reached on commercial (540) 653-(b) (6) or DSN 2(b) (6)

[redacted]

Enclosure

Copy to:
USACOM J631B

Joint Warfare Analysis Center Comments

ENCLOSURE

Recommendation #1: Complete the assessment for determining the year 2000 compliance status of all mission-critical systems.

We concur with the recommendation. The assessment for determining the year 2000 compliancy of the mission-critical systems is complete. In addition, JWAC has a plan of actions and milestones with 30 September 1998 as the date for completion of the assessment phase for all JWAC software.

Recommendation #2: Certify and document all internally managed compliant systems.

We concur with the recommendation. JWAC established an initial Y2K compliant testing environment and begun testing to validate internally managed systems. All validation results will be documented using the Year 2000 Compliancy Checklist provided in the DoD Y2K Management Plan and the ACOM Y2K Management Plan. Scheduled completion of validation for internally managed systems is 31 October 1998.

Recommendation #3: Develop contingency plans for all mission-critical systems that are not scheduled to be compliant by 31 December 1998.

We concur with the recommendation. JWAC is developing contingency plans for all mission-critical systems which will not be compliant by 31 December 1998 and is scheduled for completion 1 November 1998. Contingency plans for the remaining mission-critical software is scheduled for completion by 31 December 1998.

Enclosure A

Joint Warfighting Center Comments

JOINT WARFIGHTING CENTER
FENWICK ROAD BLDG 96
FORT MONROE VIRGINIA 23651-5000

24 September 1998

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL,
ATTN: MR THOMAS F. GIMBLE, DIRECTOR, ACQUISITION
MANAGEMENT DIRECTORATE

SUBJECT: Audit Report on the Joint Centers' Year 2000 Issues
(Project No. 8AS-0006.05)

1. The Joint Warfighting Center (JWFC), FT Monroe, continues aggressive management of the Year 2000 (Y2K) program. The JWFC, FT Monroe, is transitioning from the Joint Staff to the United States Atlantic Command effective 1 Oct 98. The Center has already merged with USACOM/J7 and the Joint Training, Analysis and Simulation Center (JTASC) in Suffolk. The merged organization is called the USACOM JWFC. The JTASC/JWFC Y2K programs have already been merged. The status of the merged Y2K program is reported regularly to the USACOM Y2K program management office.

2. Within the context of the merger described above, the original list of JWFC Mission Critical Systems has been reviewed. The review results show that none of the JWFC systems are USACOM mission critical. USACOM JWFC has adopted a Training Critical definition. Six (6) of the original 19 JWFC mission critical systems meet the Training Critical definition.

3. The six JWFC Training Mission Critical systems have been assessed for Y2K compliance. The certification and documentation of all internally managed compliant systems continues.

4. Specific comments concerning the draft audit report "Recommendations for Corrective Action" are provided within the enclosure.

M. R. BERNDT
Major General, USMC
Commander

Enclosure

Joint Warfighting Center Comments

The Joint Warfighting Center Year 2000 Program

Recommendations for Corrective Action

1. We recommend that the Commander, Joint Communications Support Element; Commander, Joint Command and Control Warfare Center; Commander, Joint Warfare Analysis Center; and Commander, Joint Warfighting Center take immediate action to:

a. Complete the assessment for determing the year 2000 compliance status of all mission critical systems. **Concur. Completed. None of the JWFC systems are ACOM Mission Critical. The JWFC, FT Monroe Training Critical systems fall into two general categories, those that are currently in use and those that are under development. The table shown below provides the current status of these systems. The assessment was completed in August 1998.**

	Compliant	Noncompliant	Unknown	Total/Remarks
Systems in use (Phase III, Validation)	3 (JTLS, JEL, JCLL)	0	0	3
Systems under development	3 (IDPS, JCATS, JEMP III)	0	0	3
Total	6	0	0	6

b. Certify and document all internally managed compliant systems. **Concur. JWFC continues to process all internally managed systems through the Y2K Program phases of Renovation, Validation and Implementation. Estimated completion date is March 1999.**

c. Develop contingency plans for all mission-critical systems that are not scheduled to be compliant by December 31, 1998. **Concur. As stated above, none of the JWFC systems are considered ACOM mission critical. Training Critical System Contingency Plans will be developed, as they are needed.**

Audit Team Members

This report was prepared by the Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD.

(b) (6)