Audit Report

SUMMARY OF DOD YEAR 2000 AUDIT
AND INSPECTION REPORTS II

Report No. 99-115 March 29, 1999

Office of the Inspector General
Department of Defense

Additional Information and 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 Audit Followup, and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

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

Defense Hotline

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

Acronym

Y2K	Year 2000

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

March 29, 1999

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)

SUBJECT: Summary of DoD Year 2000 Audit and Inspection Reports II (Report No. 99-115)

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

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

Questions on the report should be directed to Mr. Timothy J. Harris at (703) 604-9053 (DSN 664-9053) (tharris@dodig.osd.mil) or Ms. Mary L. Ugone at (703) 604-9049 (DSN 664-9049) (mlugone@dodig.osd.mil). See Appendix D 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. 99-115 **March 29, 1999**
(Project No. 8AS-0032.22)

Summary of DoD Year 2000 Audit and Inspection Reports II

Executive Summary

Introduction. This report summarizes 43 audit and inspection reports, memorandums, and briefings pertaining to DoD organizations and their year 2000 conversion progress. The reports were issued from October 1998 through February 1999.

Results. Year 2000 conversion problems were identified within the following areas:

- oversight (6 reports)
- reporting (10 reports)
- assessment (9 reports)
- resources (6 reports)
- interfaces (10 reports)
- prioritization (3 reports)
- testing (15 reports)
- contingency and continuity of operations planning (23 reports)
- contracts (6 reports)
- infrastructure (6 reports)

The DoD has made significant progress in addressing year 2000 issues and problems, especially in the last few months. Specifically, DoD has reported a substantial increase in the percentage of compliant mission-critical systems and systems that completed the renovation, validation and implementation phases. In addition, various organizations and functional proponents are taking extra steps to ensure that their respective systems will be year 2000 compliant and core processes will continue to operate after December 31, 1999. However, audit results indicate that DoD must continue its aggressive action to ensure that adequate testing is conducted and realistic contingency plans are developed to mitigate year 2000 risks. Other issues that continue to challenge DoD include a significant remaining number of noncompliant mission-critical systems, including systems for such sensitive areas as force management and chemical demilitarization; host nation support; supplier outreach; and mainframe computer compliance.

Management Comments. Although no comments were required, the Principal Director, Year 2000 recommended that this report address the difference between system contingency and operational contingency plans in the matrix of year 2000 issues shown in Appendix A.

Audit Response. We did not identify the difference between system contingency and operational contingency plans for this report because relevant governing criteria was not fully in effect during the timeframe that the audits and inspections listed in the matrix of year 2000 issues (Appendix A) were conducted. However, for subsequent summary reports, we might be able to portray shortfalls in system contingency and operational contingency plans, if the audit and inspection reports identify issues related to each type of contingency plan.

Table of Contents

Executive Summary i

Introduction

Background 1
Objectives 2

Finding

Indicators of Year 2000 Progress 3

Appendixes

A. Matrix of Year 2000 Issues 12
B. Summaries of Year 2000 Audit and Inspection Reports, Briefings, and Memorandums 17
C. Year 2000 Memorandums 37
D. Report Distribution 39

Management Comments

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments 42

Background

Complexity of the Year 2000 Challenge. The task of ensuring there is no significant impairment of the DoD ability to execute its missions and day-to-day functions is one of the most complex challenges ever faced by DoD managers. This is primarily because of the sheer magnitude of the problem. Of particular note:

- DoD uses about 28,000 information systems, of which approximately 2,300 are mission-critical,
- hundreds of thousands of pieces of equipment, ranging from the largest weapon systems to hand-held electronics, contain tens of millions of microprocessor chips, some of which are date sensitive, and
- when U.S. forces deploy, they depend on allies and host nations for a wide range of additional logistical support services, as specified in thousands of agreements with dozens of governments.

In addition, the DoD year 2000 (Y2K) conversion challenge has been made considerably more difficult by a combination of factors related to management culture. Those factors include:

- A legacy of very decentralized information technology resources management, which led to a runaway proliferation of systems that was only recently addressed.
- An initial tendency to view the millennium bug as a purely technical problem that could be solved by the information technologists, without a need for much involvement by managers and commanders.

Audit and Inspection Community Role. The Inspector General, DoD, and the DoD Chief Information Officer formed an informal partnership in early 1997 to help achieve sufficient oversight and management control in those areas considered to have the most risk. Most other DoD audit and inspection organizations have similar agreements or taskings within their Services.

Management Action. In August 1998, the Secretary of Defense declared that DoD progress on Y2K issues had been insufficient. Both the Secretary and Deputy Secretary of Defense prescribed a number of measures to accelerate DoD efforts and to move accountability for Y2K success beyond the boundaries of the information technology community to all senior managers and commanders.

DoD Management Strategy. The Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), issued the revised "DoD Year 2000 Management Plan," version 2.0, in December 1998. The DoD Y2K Management Plan provides the overall strategy and guidance for ensuring continuance of a mission-capable force able to execute the National Military Strategy before, on, and after January 1, 2000. See Appendix C for other recently issued Y2K memorandums.

Objectives

The objective of this report is to summarize Y2K issues identified in reports issued by the General Accounting Office; Inspector General, DoD; Inspector General, Navy; and Army, Navy, and Air Force audit agencies from October 1998 through February 1999. The Inspector General, Army, and the Inspector General, Air Force, had not yet formally reported on Y2K. Appendix A provides a matrix of issues identified in the 43 reports, memorandums, and briefings that involved DoD organizations. Appendix B contains a summary of the problems identified and corrective actions recommended in each publication listed in the matrix.

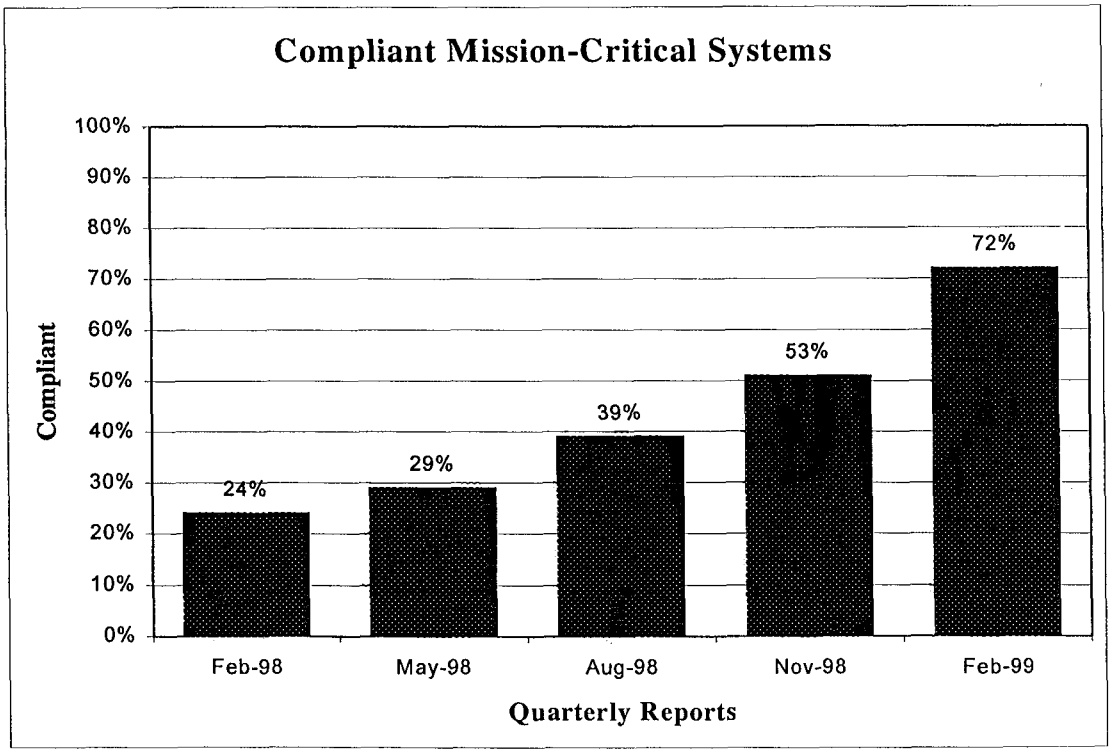
Indicators of Year 2000 Progress

The DoD made significant progress in addressing Y2K issues and problems during the last year. Specifically, DoD reported a substantial increase in the percentage of compliant mission-critical systems and systems that have completed the renovation, validation, and implementation phases. In addition, various organizations and functional proponents are taking extra steps to ensure that their respective systems will be Y2K compliant and core processes will continue to operate after December 31, 1999. However, DoD must continue its aggressive action to ensure that adequate testing is conducted and that realistic contingency plans are developed to mitigate Y2K risks. Several areas continue to pose significant challenges.

Progress Made in the Last Year

DoD made significant progress in addressing Y2K issues and problems during the last year. Specifically, DoD substantially increased the percentage of compliant mission-critical systems, and the percentage of mission-critical systems that have completed the renovation, validation, and implementation phases.

Increase in Compliant Mission-Critical Systems. In its quarterly reports to the Office of Management and Budget, DoD reported a significant increase in the percentage of compliant mission-critical systems from February 1998 through February 1999. As shown in the following graph, the percentage of compliant mission-critical systems increased 48 percent from 24 percent in February 1998 to 72 percent in February 1999.



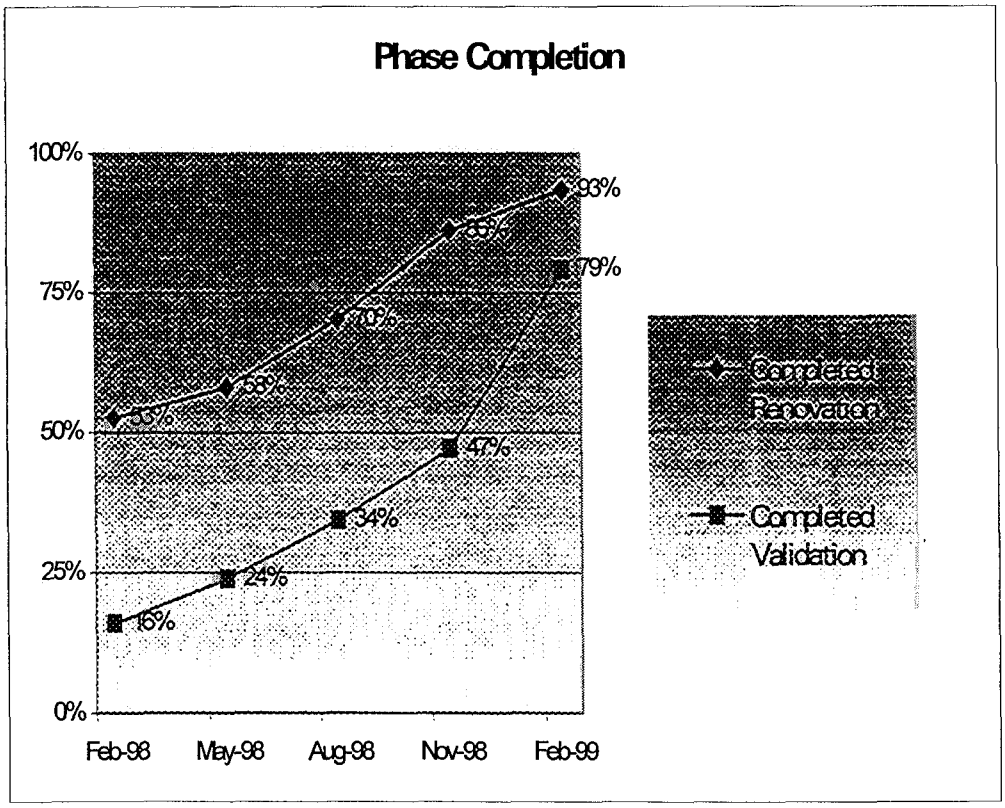
DoD Y2K Status as Reported in the February 1999 Quarterly Report. In the eighth Y2K quarterly progress report to the Office of Management and Budget, DoD reported that

> "The Department of Defense has made tremendous progress during the past quarter and substantially met its self-imposed milestone of December 31, 1998, to complete all mission-critical systems."

As of February 1999, DoD reported 2,306 active mission-critical systems, of which 1,670 are compliant, 144 are expected to be replaced or retired before the year 2000, and 492 are being repaired. Of the 492 systems still being repaired:

- 8 are in the assessment phase,
- 96 are in the renovation phase,
- 226 are in the validation phase, and
- 162 are in the implementation phase.

DoD projects that more than 90 percent of all its mission-critical systems will be compliant before March 31, 1999. This projection is supported by progress reported by DoD for systems completing the critical renovation and validation phases, as shown in the following graph.



Results of DoD Audits and Inspections

This report summarizes 43 audit and inspection reports, memorandums, and briefings, issued from October 1998 through February 1999, that discussed Y2K risk areas and identified shortfalls within various DoD Components. Specifically, the General Accounting Office (GAO), the Inspector General, DoD (DoD IG), the Army, Navy, and Air Force audit agencies, and the Inspector General, Navy (Navy IG) have issued Y2K reports, memorandums, and briefings that identified shortfalls in the following areas.

	GAO	DoD IG	Army Audit	Air Force Audit	Navy Audit	Navy IG	Total
Oversight	0	2	0	0	2	2	6
Reporting	0	1	4	0	4	1	10
Assessment	0	3	2	1	0	3	9
Resources	0	1	1	0	1	3	6
Interfaces	2	0	6	0	1	1	10
Prioritization	0	0	0	1	1	1	3
Testing	2	3	4	1	2	3	15
Contingencies	2	3	6	1	6	5	23
Contracts	0	2	2	0	2	0	6
Infrastructure	0	0	0	1	3	2	6

The percentage of reports identifying shortfalls has decreased for all risk areas compared to previous audit and inspection reports summarized in Inspector General Report, "Summary of DoD Year 2000 Conversion - Audit and Inspection Results," December 24, 1998. However, an accurate conclusion cannot be drawn from the comparison because the objectives and scope of the audits may have varied.

Examples of Significant Progress

The reports discussed in this summary identified several organizations and functional proponents that were successfully dealing with the Y2K challenge and, in some cases, developing best practices and techniques. Examples of significant progress made in Y2K conversion efforts relating to a functional area, an installation, an operational command, and a mission-critical system are discussed below.

Health Care Functional Area. The Defense Health Program must ensure that Y2K problems do not disrupt the delivery of quality care to patients. The Assistant Secretary of Defense (Health Affairs) took effective steps to mitigate the risk of Y2K related disruptions. For example, medical personnel conducted independent verification and validation of mission-critical systems, aggressively addressed biomedical device issues, and evaluated test results of biomedical device manufacturers.

Independent Verification and Validation. The Assistant Secretary of Defense (Health Affairs) has completed independent verification and validation for the 13 mission-critical automated information systems. All 13 systems were certified as Y2K compliant and site implementation was completed at 12 sites by December 31, 1998.

Biomedical Devices. Some biomedical devices will not be Y2K compliant by March 31, 1999. Because of embedded chips in many biomedical devices, manufacturers have advised hospitals and health providers not to test the devices for compliance. The Assistant Secretary of Defense (Health Affairs) has taken the position that it is still safe to use these devices until the Y2K fix is in place, and is working on a waiver process to manage this situation.

Evaluation of Test Results. Medical Logistics personnel attended American Hospital Association work group meetings that focused on evaluating test results for manufacturer biomedical devices. Teams, including Inspector General, DoD personnel, visited manufacturers to review whether the manufacturers' test support and procedures were Y2K compliant.

Dugway Proving Ground. The Dugway Proving Ground range and test facility is on schedule with renovating its business and test information systems for Y2K compliance (see Appendix B, page 20, for the summary of the report). The Army facility took positive actions to:

- develop contingency plans,
- test all systems to ensure compliance or noncompliance,
- complete all required documentation and certification forms, and
- complete the implementation phase for all mission-critical systems.

III Marine Expeditionary Force. The III Marine Expeditionary Force took a proactive approach to ensuring that its information systems will be Y2K compliant. The III Marine Expeditionary Force assessed system compliance, implemented corrective actions, and accurately reported the status of issues concerning potential Y2K-related failures. In addition, III Marine Expeditionary Force officials appointed a Y2K Operational Evaluation planner to design a Y2K test scenario, which will be coordinated with Marine Corps headquarters, other Marine Expeditionary Forces, and Marine forward-deployed activities. As a result of these efforts, when the III Marine Expeditionary Force Y2K conversion effort is completed, risk of mission capability impairment because of Y2K problems should be low (See Appendix B, page 18, for the summary of the report).

Advanced Field Artillery Tactical Data System. The Army Audit Agency reported that the Advanced Field Artillery Tactical Data System is at low risk of Y2K failure (see Appendix B, page 23, for the summary of the report). The program office for the Advanced Field Artillery Tactical Data System effectively identified and managed technical-resource and time-risk areas. In addition, the Advanced Field Artillery Tactical Data System participated in the Y2K sensor-to-shooter demonstration conducted at the White Sands Missile Range in New Mexico. During the Y2K test, the Advanced Field Artillery Tactical Data System successfully transmitted digital and voice commands for fire support from the Apache Attack and the Kiowa Warrior Helicopters. After the test, the Army Y2K coordinator stated, "This clearly shows that we are ready to be deployed rapidly, and that we will be able to do our job."

Contingency Plans and Testing

Although DoD made progress in addressing Y2K challenges, contingency planning and testing remain as difficult areas that require intensive management.

Contingency and Continuity-of-Operations Plans. Contingency and continuity-of-operations planning is necessary to ensure that mission-critical functions will continue to operate in the event of Y2K failures. Of the 23 audit and inspection reports that identified shortfalls in contingency and continuity-of-operations planning:

- 8 did not have contingency plans,
- 8 did not have neither contingency plans nor continuity-of-operations plans, and
- 7 had inadequate contingency plans or continuity-of-operations plans.

The General Accounting Office issued AIMD 10.1.19, "Year 2000 Computing Crisis: Business Continuity and Contingency Planning," August 1998 to assist agencies with their contingency planning. The guide provides a framework for agencies to manage the risk of potential Y2K-induced disruptions and provides information on the scope and challenge of continuity and contingency planning efforts.

In addition, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) has developed a web site to assist contingency planners. The following web site contains useful resources oriented toward contingency planning.

http://www.c3i.osd.mil/org/cio/y2k/y2k_con_plan/index.html

For example, the web site contains a matrix of planning assumptions to help focus resources on those potential disruptions that are most likely to occur and cause dramatic impacts. The web site will also be used to solicit best practices and lessons learned from successful management contingency strategies.

The Inspector General, DoD, announced an audit on January 13, 1999, of selected systems that were certified as Y2K compliant. As part of the audit, contingency plans will be reviewed to determine whether an adequate contingency plan exists to ensure continuity of operations.

Testing. Complete and thorough Y2K certification testing is essential to provide reasonable assurance that systems will process dates correctly and will not jeopardize an organization's ability to perform core business operations. The DoD is planning to conduct military Y2K operational evaluations and end-to-end tests of its mission-support capabilities to verify operational readiness and meet statutory requirements.

The National Defense Authorization Act for FY 1999 requires DoD to evaluate Y2K compliance as part of training exercises. Specifically, DoD must conduct Y2K testing in at least 25 military exercises, and at least 2 of the exercises must be conducted by the commander of each unified or specified combatant command. In addition, all mission-critical systems that are expected to be used during a major theater of war must be tested in at least two exercises. However, the Act states that if the required testing is not feasible or presents undue risk, functional end-to-end tests may be used.

In addition to certification testing, various DoD Components are engaged in the following three kinds of "higher level" testing:

- Intersystem integration testing at the Military Service or lower organizational levels,
- End-to-end system tests covering processes across functional areas, such as finance or command and control, and
- Operational evaluations by the unified commands around the world.

Previous audits and inspections focused on Y2K certification testing. Of the 15 audit and inspection reports that identified shortfalls in testing:

- 6 stated that no testing plans had been prepared,
- 5 stated that testing performed was inadequate,
- 2 stated that Y2K certifications were incomplete, and
- 2 stated that systems would not be ready for end-to-end testing.

The General Accounting Office issued AIMD 10.1.21, "Year 2000 Computing Crisis: A Testing Guide," November 1998, to assist agencies with their testing process. The guide presents a step-by-step framework for managing all Y2K testing activities, including those activities associated with vendor-supported systems or system components.

Other Potential High-Risk Issues

Other issues that continue to challenge DoD include:

- a significant remaining number of noncompliant mission-critical systems, including systems for such sensitive areas as force management and chemical demilitarization;
- host nation support;
- supplier outreach; and
- mainframe computer compliance.

Remaining Noncompliant Mission-Critical Systems. As of February 1999, well over 600 mission-critical systems remain noncompliant, including systems for such sensitive areas as force management and chemical demilitarization.

Force Management. Force management systems are critical for the efficient and effective employment of resources (personnel and equipment) for military or other emergency requirements. Force management systems include command and control systems as well as battle management systems, some of which are not yet compliant. For example, the Global Command and Control System – Maritime and the Theatre Battle Management Core System are not expected to be compliant until after September 1999. Optimal movement and placement of U.S. forces may be impacted if force management systems are not Y2K ready.

Chemical Demilitarization. Chemical demilitarization facilities face increased risk of mission impairment because mission-critical systems are not expected to be compliant until late 1999. For example, the Johnston Island Chemical Demilitarization Facility Control System and the Tooele Utah Chemical Demilitarization Facility Control System have been acknowledged by DoD as high-risk systems because they remained noncompliant. Audits conducted at the Tooele and Johnston Atoll chemical disposal facilities found that the Y2K managers were not making timely progress in assessing mission-critical systems for Y2K compliance, and had not prepared necessary Y2K documentation (see Appendix B, page 19 and page 21, for summaries of the reports). Chemical demilitarization facilities are responsible for the safe destruction of all chemical warfare agents, including nerve gas and blister agents. The demilitarization facilities use systems that monitor air quality within the buildings and transmit date-sensitive data to a plant control system. At the time the audits were conducted, none of the air monitoring systems were Y2K compliant. Successful completion of all Y2K conversion actions is necessary to avoid operational

impairment, including shutdown, and obviate any safety concerns. After the audits, the Army intensified its management oversight and reported that the schedule for attaining compliance would be accelerated.

Host Nation Support. Host nation support is an area of special concern because of DoD dependence on communication systems and infrastructure support supplied by host nations. Audits indicate that additional effort is needed to ensure that nations hosting DoD organizations have the ability to conduct successful operations. Availability of Y2K data on host-nation infrastructure and guidance on addressing the issue is limited; therefore, audit work is currently underway at the U.S. Pacific Command, the U.S. Central Command, and the U.S. European Command.

Supplier Outreach. DoD faces an increased risk of production and delivery disruptions because of belated focus on outreach to suppliers to ensure Y2K conversion is completed. If mission-critical information or products are not available to DoD because external suppliers are not Y2K compliant, logistics disruptions could occur. The Joint Supplier Capability Working Group has been established to develop a more systematic assessment of the critical suppliers' Y2K compliance. A sustained effort by the Military Departments and Defense Logistics Agency is needed to compensate for the belated focus and to ensure a proper evaluation of the critical suppliers' ability to provide critical items into the year 2000 and beyond.

Mainframe Computer Compliance. Defense Megacenter mainframe computers merit intensive management attention and particularly thorough Y2K-compliance testing because of their critical role in DoD computing, especially in support of finance, personnel, and logistics functions.

Conclusion

Audit results and management reporting indicate that DoD has made significant progress in addressing year 2000 issues and problems. DoD has reported a substantial increase in the percentage of compliant mission-critical systems that completed the renovation, validation, and implementation phases. In addition, various organizations and functional proponents are taking extra steps to ensure that their respective systems will be Y2K compliant and core processes will continue to operate after December 31, 1999. However, audit results also indicate that much work remains to be done. In particular, DoD must continue its aggressive action to ensure that adequate testing is conducted and realistic contingency plans are developed to mitigate Y2K risks. A significant number of noncompliant mission-critical systems and other areas continue to require intensive management.

Management Comments on the Finding and Audit Response

Management Comments. Although no comments were required, the Principal Director, Year 2000 recommended that this report address the difference between system contingency and operational contingency plans in the matrix of year 2000 issues shown in Appendix A.

Audit Response. We did not identify the difference between system contingency and operational contingency plans for this report because relevant governing criteria was not fully in effect during the timeframe that the audits and inspections listed in the matrix of year 2000 issues (Appendix A) were conducted. However, for subsequent summary reports, we might be able to portray shortfalls in system contingency and operational contingency plans, if the audit and inspection reports identify issues related to each type of contingency plan.

Appendix A. Matrix of Year 2000 Issues

Report No.	Organization/ Function/System	Ap.B Page	Over-sight.	Report.	Assess.	Resour.	Interf.	Priorit.	Testing	Cont.& Coop.	Contcts.	Infrast.	No Issues
General Accounting Office													
Briefing Report January 29, 1999	Y2K Remediation Efforts of Mission-Critical Systems						X		X	X			
Memorandum	Simulated Y2K Exercises								X				
AIMD 99-20	New Civilian Personnel System						X			X			
Inspector General, DoD													
99-086	III Marine Expeditionary Force												X
99-085	Hawaii Information Transfer System										X		
99-082	Defense Automatic Addressing System									X	X		
99-081	Tooele Chemical Agent Disposal Facility		X		X				X	X			
99-079	Dugway Proving Ground												X
99-076	Mid-Tier Computer Systems												X
99-074	Atlantic Fleet Weapons Training Facility		X										

Report No.	Organization/ Function/System	Ap.B Page	Over-sight.	Report.	Assess.	Resour.	Interf.	Priorit.	Testing	Cont.& Coop.	Ctracts.	Infrast.	No Issues
99-070	Hill, Patrick, Holloman, and Vandenberg Bases												X
99-063	Global Positioning System				X	X			X				
99-060	Johnston Atoll Chemical Agent Disposal System			X	X				X	X			
Army Audit Agency													
AA 99-121	Apache Attack Helicopter at the Office of the Program Executive Officer for Air and Missile Defense			X			X						
AA 99-122	Patriot Missile System at the Office of the Program Executive Officer for Air and Missile Defense			X			X				X		
AA 99-719	Office of the Program Executive Officer for Command, Control and Communications												X
AA 99-720	Joint Program Office for Biological Defense								X	X			
AA 99-721	Counter Narcotics Command and Management System				X		X			X			

Report No.	Organization/ Function/System	Ap.B Page	Over-sight.	Report.	Assess.	Resour.	Interf.	Priorit.	Testing	Cont.& Coop.	Ctracts.	Infrast.	No Issues
AA 99-722	Program Executive Officer Standard Army Management Information Systems			X		X	X		X	X			
AA 99-723	Reserve Component Automation System				X				X	X	X		
AA 99-28	U.S. Army Air Traffic Control Activity						X			X			
AA 99-29	Program Executive Officer for Command, Control and Communications Systems						X		X	X			
AA 99-30	Army Legacy Air Traffic Control Mission-Critical Systems			X									
Inspector General, Navy													
Not Numbered	Chief of Naval Education and Training			X			X			X			
Not Numbered	Potential Loss of Operational Readiness and Confidence		X						X				
Not Numbered	Facilities and Infrastructure Assessment				X	X							
Not Numbered	Communications/ Information Technology Management Deficiencies							X		X		X	

Report No.	Organization/ Function/System	Ap.B Page	Over-sight.	Report.	Assess.	Resour.	Interf.	Priorit.	Testing	Cont.& Coop.	Ctracts.	Infrast.	No Issues
Not Numbered	Continuity of Naval Intelligence Operations and Theater Dependencies									X			
Not Numbered	Y2K Remediation for Foreign Military Sales		X						X				
Not Numbered	U.S. Atlantic Fleet				X								
Not Numbered	U.S. Naval Forces Europe					X						X	
Not Numbered	Commander-in-Chief U.S. Pacific Fleet								X	X			
Not Numbered	Chief of Naval Operations				X	X				X			
Naval Audit Service													
Memorandum	Naval Research Laboratory												X
Memorandum	Naval Surface Warfare Center Dahlgren Division									X			
Memorandum	Strategic Systems Programs								X	X		X	
Memorandum	Naval Sea Systems Command's SEA-08 Nuclear Propulsion												X
Memorandum	Bureau of Medicine and Surgery		X	X								X	

Report No.	Organization/ Function/System	Ap.B Page	Over-sight.	Report.	Assess.	Resour.	Interf.	Priorit.	Testing	Cont.& Coop.	Ctracts.	Infrast.	No Issues
Memorandum	Military Sealift Command			X						X	X	X	
Memorandum	Norfolk Naval Shipyard		X					X		X	X		
Memorandum	Naval Sea Systems Command Headquarters			X		X			X	X			
Memorandum	Naval Air Systems Command			X			X			X			
Air Force Audit Agency													
Briefing Report	Major Commands				X			X	X	X		X	

Acronym List

Ap.B Page	Appendix B Page Reference
Report.	Reporting
Assess.	Assessment
Resour.	Resources
Interf.	Interfaces
Priorit.	Prioritization
Cont. & Coop.	Contingency and Continuity-of-Operations Planning
Ctracts.	Contracts
Infrast.	Infrastructure

Appendix B. Summaries of Year 2000 Audit and Inspection Reports, Briefings, and Memorandums

Following are summaries of the Y2K issues detailed in audit and inspection reports, briefings, and memorandums. At the end of each summary, we describe the recommendations[1] made and the status of any agreed-upon management actions.

General Accounting Office

"Briefing on Year 2000 Remediation Efforts of Mission-Critical Systems," January 29, 1999. The General Accounting Office presented a briefing to the House Appropriations Committee Subcommittee on Defense on the status of six systems[2] that were reported at risk in December 1998. Specifically, the following systems were deemed at risk based on project risk factors:

- Defense Switch Network,
- Fleet Satellite Communications Systems,
- Global Command and Control System,
- Global Combat Support System,
- Global Positioning System, and
- Joint Total Asset Visibility System.

Defense Switch Network. The General Accounting Office found that the Defense Switch Network was behind schedule and that switch upgrades at Air Force and Army bases were planned for September 1999. In addition, tests performed by the Joint Interoperability Test Command were not independently verified, and detailed Y2K contingency plans were not completed.

Fleet Satellite Communications Systems. The Fleet Satellite Communications Systems had mission-critical components that did not meet Y2K validation phase and implementation phase completion dates. However, contingency plans were finalized.

[1] The summaries do not include all recommendations made in the reports. In most cases, the summaries include only those recommendations that directly apply to the shortfall areas discussed in Appendix A.

[2] The systems are 6 of the top 20 DoD mission-critical systems.

Global Command and Control System. The Global Command and Control System did not meet the DoD mission-critical milestone date for the validation phase. In addition, all system interfaces were not fully tested and certified.

Global Combat Support System. The Global Combat Support System's Y2K risk-management and contingency plans were not yet developed. System certification was completed, but not approved. Integration and end-to-end testing should be completed by March 31, 1999.

Global Positioning System. The Global Positioning System did not complete Y2K remediation as mandated by the DoD Y2K Management Plan. In addition, the General Accounting Office found limited testing of Global Positioning System receivers, unidentified end-to-end testing strategies, and unscheduled acceptance testing.

Joint Total Asset Visibility System. The Joint Total Asset Visibility System had draft continuity of operations and contingency plans. However, although the system was reported as Y2K certified, there was no certification documentation.

Memorandum to Congressional Committees, "Defense Computers: DoD's Plan for Execution of Simulated Year 2000 Exercises," January 29, 1999. The memorandum states that as of January 29, 1999, DoD had not submitted a plan to Congress for the execution of simulated Y2K exercises. The DoD Appropriations Act and the Strom Thurmond National Defense Authorization Act for FY 1999 required DoD to submit a formal plan by December 15, 1998. However, DoD was working on an overall operational evaluation plan, and the unified commands planned to conduct 31 operational evaluations through September 1999. Initial evaluations at the North American Aerospace Defense Command and the Strategic Command had been conducted. The strategy for performing future DoD Y2K work entails assessing selected operational evaluations and related activities. The General Accounting Office was to brief the congressional committees on the results of the assessments as they were completed.

Report No. AIMD-99-20 (OSD Case No. 1719), "Alternative Should Be Considered in Developing the New Civilian Personnel System," January 27, 1999. The report states that the DoD did not adequately address risks associated with the Y2K computing problem for the Defense Civilian Personnel Data System. Specifically, DoD did not develop adequate interface agreements and contingency plans. Civilian personnel business operations are at risk of Y2K disruptions caused by external interfacing systems and the public infrastructure. The report recommended that DoD:

- Establish interface agreements that clearly specify date-format changes, timeframes for the changes, and processes for resolving conflicts;

- Refine business continuity and contingency plans to ensure that they consider risks posed by external systems and infrastructure; assess the costs and benefits of alternative contingency strategies; and describe the resources, staff roles, procedures, and timetables needed to implement the plan; and
- Test contingency plans to ensure that they are capable of providing the desired level of support to the agency's core business processes and can be implemented within a specified period of time.

DoD concurred with the recommendations and stated that the Defense Civilian Personnel Service had interface agreements in place, had issued a contingency management manual, and would ensure that Component plans included a requirement to test contingency processes.

Office of the Inspector General, DoD[3]

Inspector General, DoD, Report No. 99-086, "Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility – III Marine Expeditionary Force," February 22, 1999. The report states that the III Marine Expeditionary Force had taken a proactive approach to ensuring that its information systems would be Y2K compliant. The III Marine Expeditionary Force took several positive actions including assessing and coordinating Y2K compliance and tracking and assessing progress of all categories of systems, computers, and communication devices. When the III Marine Expeditionary Force Y2K conversion effort is completed, risk of impaired mission capability should be low.

Inspector General, DoD, Report No. 99-085, "Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility – Hawaii Information Transfer System," February 22, 1999. The report states that the Hawaii Information Transfer System program managers, the Defense Information System Agency, and the Naval Computer and Telecommunications Area Master Station-Pacific recognized the need for contract clauses and procedures to ensure Y2K compliance for the program. The system contractor was required to ensure that all hardware and software assets were Y2K compliant and that the contract specified there could be no additional charges to the Government for Y2K upgrades. Further, the implementation of the Hawaii Information Transfer System Y2K upgrades to existing systems was on schedule.

Inspector General, DoD, Report No. 99-082, "Year 2000 Computing Issues Related to the Defense Automatic Addressing System Center," February 18, 1999. The Defense Logistics Agency and the Defense Automatic Addressing System Center recognized the importance of the Y2K issue and have taken several positive actions to identify and correct Y2K problems in its automated information systems. However, the Defense Automatic Addressing System

[3] The full text of Inspector General, DoD, reports is available on the Internet at http://www.dodig.osd.mil and summaries of Y2K audit activity are accessible at http://www.ignet.gov.

Center needs to improve its contingency plan and incorporate Federal Acquisition Regulation Y2K requirements in contracts for automated information systems to ensure that the Defense Logistics Agency will be able to perform its core supply mission without interruption. The Defense Automatic Addressing System Center draft contingency plan did not fully address the DoD Y2K Management Plan requirements and guidelines for risk management and contingency planning. Furthermore, the draft plan did not contain alternative procedures for working around system failures and did not describe how the Defense Automatic Addressing System Center would preserve data, such as backing up the systems. The contingency plan needs to address alternative procedures for continuity of operations of the core mission and to describe how the Defense Automatic Addressing System Center would preserve data for its mission-critical Automated Information Systems.

In addition, the Defense Automatic Addressing System Center did not address Federal Acquisition Regulation Y2K requirements in information technology contracts for maintenance and software development.

The report recommended that the Director, Defense Automatic Addressing System Center:

- prepare contingency plans in accordance with the requirements and guidelines in the DoD Y2K Management Plan to include addressing workarounds and data preservation.
- include Federal Acquisition Regulation Y2K compliance language in all open contracts for the purchase of information technology products, including software.

The Defense Logistics Agency concurred with the recommendations and stated that the Defense Automatic Addressing System Center had added data preservation strategies and workarounds to its contingency plans. Also, the Defense Logistics Agency stated that compliance language was included in all contracts before January 31, 1999.

Inspector General, DoD, Report 99-081, "Tooele Chemical Agent Disposal Facility Preparation for Year 2000," February 16, 1999. The report states that the Project Manager for Chemical Stockpile Disposal at the Tooele Chemical Agent Disposal Facility did not make timely progress assessing the information technology systems. In addition, he did not prepare the necessary Y2K documentation, specifically, the assessment plan, the contingency plan, the risk-management plan, and the validation plan and schedule as required by the DoD Y2K Management Plan. In addition, the Army Program Manager for Chemical Demilitarization at Aberdeen Proving Ground did not provide oversight and emphasis by visiting the Tooele Facility to determine the Y2K status and verify the accuracy of the progress in making the Tooele systems Y2K compliant. As a result, the facility was badly behind schedule for Y2K conversion.

The report recommended that the Army Program Manager for Chemical Demilitarization at Aberdeen Proving Ground:

- Establish a schedule to identify and correct Y2K solutions for affected systems at the Tooele Chemical Agent Disposal Facility;
- Require the Project Manager for Chemical Stockpile Disposal at the Tooele Chemical Agent Disposal Facility to prepare an assessment plan, a contingency plan, a risk-management plan, and a validation plan and schedule; and
- Establish a visitation schedule for the Tooele Chemical Agent Disposal Facility for timely assessment of the Y2K problem and implementation of necessary corrections.

The Deputy Assistant Secretary of the Army for Chemical Demilitarization concurred with all recommendations, and the Army has made significant progress in addressing the Y2K challenge at the Tooele Chemical Stockpile Disposal facility.

Inspector General, DoD, Report No. 99-079, "Year 2000 Conversion Program at the Dugway Proving Ground Major Range and Test Facility," February 9, 1999. The report states that the Dugway Proving Ground range and test facility was on schedule with renovating its business and test information systems for Y2K compliance. The Dugway Proving Ground identified seven systems for assessment, developed contingency plans, tested all systems to ensure Y2K compliance, and maintained all necessary documentation.

Inspector General, DoD, Report No. 99-076, "Year 2000 Posture of DoD Mid-Tier Computer Systems," February 3, 1999. The report states that the managers of the 14 mid-tier systems reviewed were actively managing each primary element to achieve Y2K compliance, and that they appropriately reported the Y2K status of each mission-critical computer system. The primary reason that mid-tier systems were appropriately managed and reported was because the primary elements of each system were the responsibility of a single manager. For the mid-tier systems reviewed, the risk of system failure because of a primary element being overlooked was low.

Inspector General, DoD, Report No. 99-074, "Year 2000 Conversion at the Atlantic Fleet Weapons Training Facility," January 29, 1999. The report states that the Atlantic Fleet Weapons Training Facility did not begin or complete its Y2K resolution process in a timely manner and that its operating systems may not be Y2K compliant. The Atlantic Fleet Weapons Training Facility uses operating systems that may not be Y2K compliant because of the lack of oversight, guidance, coordination, and awareness from command-level senior management. Most of the Naval Command's 13 software systems were behind schedule in meeting the Navy Y2K Action Plan milestones for the awareness, assessment, and renovation phases and will not meet the validation milestone. As a result, the Atlantic Fleet Weapons Training Facility is at an increased risk of not having its systems Y2K compliant by March 1999.

The report recommended that the Commander, Atlantic Fleet Weapons Training Facility:

- Develop procedures and create milestones to ensure compliance with the Department of the Navy Y2K Action Plan.
- Establish Memorandum of Agreements or similar documents for the 13 systems owned by other Naval Commands to establish responsibility and timeframes for system Y2K compliance.

The Commander, Atlantic Fleet Weapons Training Facility, concurred with the recommendations and established procedures to ensure that their systems would be Y2K compliant.

Inspector General, DoD, Report No. 99-070, "Year 2000 Conversion Program at Hill, Patrick, Holloman and Vandenberg Air Force Bases," January 22, 1999. The report states that the four Air Force bases developed their inventory, tested all their systems to ensure compliance, and maintained all the necessary documentation. The Air Force bases were making positive progress to become Y2K compliant.

Inspector General, DoD, Report No. 99-063, "Global Positioning System Receiver Compliance with Year 2000 Requirements," December 31, 1998. The report states that the Global Positioning program office did not complete the inventory and assessment of nonvalidated receivers[4] procured directly by DoD organizations, civilian Federal agencies, DoD contractors, and allied nations. The delay was partially caused by lack of cooperation by many of those organizations. In addition, DoD did not mitigate Y2K risks in testing commercial receivers. As a result, systematic distribution of information to users on equipment Y2K compliance has been hampered, increasing the risk of mission disruption.

The report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) direct the Global Positioning System joint program office, in coordination with the U.S. Coast Guard, to conduct Y2K testing on all nonvalidated receivers. The Deputy Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with the finding, but initially did not concur with the recommendations. This position was later reversed.

Inspector General, DoD, Report No. 99-060, "Johnston Atoll Chemical Agent Disposal System Preparation for Year 2000," December 24, 1998. The report states that the Army Project Manager for Chemical Stockpile Disposal did not make timely progress in assessing the information technology subsystems of the Johnston Atoll Chemical Agent Disposal System and did not prepare the necessary Y2K documentation, such as the assessment plan, the contingency plan, the risk management plan, and the validation plan and schedule, as required by the DoD Y2K Management Plan. Further, the Army Program Manager for Chemical Demilitarization at Aberdeen Proving Ground, Maryland, incorrectly

[4] Receivers are part of the of the Global Positioning System's user segment that functions with satellites to provide navigational positioning for military and civilian use.

reported the subsystem status in the monthly report to DoD. As a result, the Y2K conversion program for this facility is well behind the prescribed schedule.

The report recommended that the Army Program Manager for Chemical Demilitarization establish a schedule to identify and correct Y2K problems for systems at Johnston Atoll, require the project manager at Johnston Atoll to prepare an assessment plan, contingency plan, risk management plan, and a validation plan and schedule, and correct the monthly report to DoD by indicating that the Process Data Acquisition Reporting System is not Y2K compliant. The Army Program Manager for Chemical Demilitarization did not comment on the draft report, but did comment on the final report and concurred with all the recommendations.

Army Audit Agency

Memorandum Report AA 99-121, "Audit of Mission-Critical Systems – Year 2000 (Phase V); Assessment of the Apache Attack Helicopter at the Office of the Program Executive Officer for Aviation," January 8, 1999. The report states that Project Management Office personnel for the Apache, the Apache Longbow, and the Longbow Apache-Fire Control Radar effectively identified, monitored, traced, and resolved critical Y2K risks. The actions taken will ensure Y2K compliance of the Apache Attack Helicopter and Fire Control Radar. However, one risk area was identified. The Army's Y2K database did not reflect all systems that interfaced with the Apache Helicopter. The Program Executive Officer, Aviation, agreed to take action to update the database to reflect Apache system interfaces.

Memorandum Report AA 99-122, "Audit of Mission-Critical Systems – Year 2000 (Phase V); Assessment of the Patriot Missile System at the Office of the Program Executive Officer for Air and Missile Defense," January 8, 1999. The report states that Project Management Office personnel for the Patriot Missile System were effectively identifying, monitoring, and tracking Y2K risks. However, several risk areas required immediate management attention. Specifically, some existing contracts for the Patriot Missile System did not have the required Y2K contract language. In addition, the Tactical Command System communication processor, one of the Patriot Missile System's components, was not Y2K compliant. If the Tactical Command System's communication processor is rendered inoperable, Service communication will be impaired with targeting sensors. Further, the Army's Y2K database did not accurately reflect the status of the Patriot Missile System's Patriot Advanced Capability 2 and 3.

The report recommended that the Program Executive Officer, Air and Missile Defense, update the Army's Y2K database to reflect the accurate status of the Patriot Advanced Capability 2 and 3, and direct responsible personnel to expedite action to ensure that all new and existing contracts for the Patriot include Y2K required language. In addition, the report recommended that the Project Manager for the Patriot Missile System develop and document a risk management plan for

the Tactical Command System's communication processor in accordance with the Army Y2K Action Plan. The Program Executive Officer and the Project Manager agreed with the recommendations.

Memorandum Report No. AA 99-719, "Audit of Automated Information Systems – Year 2000 (Phase IV); Assessment of Selected Mission-Critical Systems at the Office of the Program Executive Officer for Command, Control, and Communications Systems, December 22, 1998. The report states that users of the Advanced Tactical Data System are at low risk of potentially losing continuity of operations because of Y2K problems. Program Executive Office and Project Management Office personnel were effectively identifying and managing technical, resource, and time-risk areas for the Advanced Tactical Data System. Specifically, responsible personnel:

- accurately reported the progress of the system in the Army's Y2K database,
- prepared and had both parties sign all system interface agreements, and
- identified and included trigger dates in the contingency plan.

The report did not identify any high-risk or moderate-risk areas requiring management attention and contained no recommendations.

Memorandum Report AA 99-720, "Audit of Automated Information Systems - Year 2000 (Phase IV); Assessment of Selected Mission-Critical Systems at the Joint Program Office for Biological Defense," December 22, 1998. The report discusses the Y2K status of five systems managed by the Joint Program Office for Biological Defense. The report states there was reasonable assurance that three of the five systems were proceeding on time or ahead of schedule and were rated as low risk for Y2K problems. However, the report states that two of the five systems were at moderate risk of failing on or before the year 2000. Specifically, the two systems were at risk because:

- contingency plans were not prepared,
- testing results were not documented,
- the certification process was not completed, and
- signatures had not been obtained.

The report recommended that the Joint Program Office for Biological Defense update and report relevant system information in the Army's Y2K database, document test plans and results, and prepare contingency plans. The Joint Program Manager for Biological Defense agreed with the recommendations.

Memorandum Report AA 99-721, "Audit of Automated Information Systems – Year 2000 Assessment of the Counter Narcotics Command and Management System," December 22, 1998. The report states that project office personnel for the Counter Narcotics Command and Management System actively engaged in mitigating and correcting Y2K problems including establishing a Y2K management oversight program to monitor, track, and resolve Y2K issues. However, several high-risk areas required management's attention.

Specifically, the project office for the Counter Narcotics Command and Management System did not:

- complete a risk assessment for all system components,
- complete and sign all system interface agreements, and
- complete contingency planning for all known and potential risks.

The report recommended that the Project Officer for the Counter Narcotics Command and Management System should:

- perform a risk assessment for 68 commercial-off-the-shelf and government-off-the-shelf components and prioritize those components that are most essential to the overall operation of the system.
- perform integrated testing of all critical commercial-off-the-shelf products that were prioritized as high-risk components before the system is incorporated into the U.S. Southern Command's April 1999 operation evaluation.
- develop a contingency plan to address how the project office will remedy component failures, which could cause the system to fail.
- notify the Department of State through the Office of the Joint Chiefs of Staff and the Commander in Chief, U.S. Southern Command, of the significance of formalizing a memorandum of agreement.
- finalize the memorandum of agreement with Defense Information Systems Agency.

In addition, the report recommended that the Program Executive Officer for Command, Control, and Communications Systems update the Y2K database with accurate information on the status of the Counter Narcotics Command and Management System. Responsible personnel of the system agreed with the recommendations.

Memorandum Report AA 99-722, "Audit of Automated Information Systems – Year 2000 (Phase IV); Assessment of Selected Mission-Critical Systems at the Office of the Program Executive Officer Standard Army Management Information Systems," December 22, 1998. The report states that users of the Standard Army Retail System and the Unit Level Logistic Systems (Ground and Aviation) are at high-risk of losing continuity of operations. Several high-risk areas were identified that required management attention. Specifically, responsible personnel had not:

- provided reasonable assurance that all system interfaces had been identified.
- prepared detailed test plans to include critical dates requiring testing, regression testing, and end-to-end testing.
- prepared contingency plans.
- identified all funding and personnel resources for fixing, testing, and certifying the standard logistic systems.

- reported the status of the mission-critical systems accurately to the Army's Y2K database. Responsible personnel overstated the progress for the standard logistic systems.

The report recommended that responsible personnel within the Software Development Center-Lee and the Program Management Office for Integrated Logistics Systems prepare a coordinated Y2K plan and schedule, determine whether test facilities are available, identify adequate resources, and elevate all critical issues or concerns to the Program Executive Office.

Memorandum Report AA 99-723, "Audit of Automated Information Systems – Year 2000 (Phase IV); Assessment of Selected Mission-critical Systems at the Program Executive Office, Reserve Component Automation System," December 22, 1998. The report states that the Reserve Component Automation System and the Retirement Points Accounting Management System are at moderate risk of losing continuity of operations because of Y2K problems. The report identified several risk areas. Specifically, responsible personnel had not:

- conducted testing to include all pertinent critical dates to safeguard against potential system failure,
- prepared contingency plans for all known and potential risk areas, and
- provided assurance that the Reserve Component Automation System will be Y2K compliant.

In addition, the report identified a potential risk area that could corrupt the Reserve Component Automation System. The Reserve Component Automation System has a Windows NT® platform, and two of its interfaces, the Unit Level Logistics Systems – Ground and S4, have DOS platforms. The NT platform is not compatible with the DOS platform, resulting in incompatibility between the Reserve Component Automation System hardware and the Unit Level Logistics System software. System personnel agreed that the incompatibility is a potential risk area and stated that responsible personnel would address this issue.

The report recommended that the Program Executive Officer of the Reserve Component Automation System:

- accelerate the assessment of Reserve Component Automation System components and identify solutions for mitigating the risk areas.
- conduct a risk assessment and prepare contingency plans for the Reserve Automation System and the Retirements Points Management System.
- address the Windows NT® and DOS incompatibility problem for the Reserve Component Automation System hardware and the Unit Level Logistics System software.
- test all potential critical Y2K dates that could result in a potential Reserve Component Automation System failure.

- modify the Reserve Component Automation System contract to include contract specifications that will require contractor-provided equipment to be Y2K compliant.

The Program Executive Officer and Project Manager for the Reserve Component Automation System agreed with the recommendations and directed system personnel to take action to mitigate Y2K risks.

Memorandum Report No. AA 99-28, "Audit of Automated Information Systems – Year 2000 (Phase IV); Assessment of the U.S. Army Air Traffic Control Activity," October 16, 1998. The report states that the U.S. Army Aviation Center and U.S. Army Air Traffic Control Activity established effective Y2K oversight programs, and the Commanding General and Garrison Commander were actively involved in overseeing Y2K remediation efforts. However, the report identified two Y2K risk issues that may have a significant operational impact on the Army Air Traffic Control Activity. The Activity's development of operational contingency plans was rated as moderate risk and the Activity's reliance on the Federal Aviation Administration to fix, test, and certify the Automated Radar Terminal/Tracking System as Y2K compliant was identified as a high-risk area. Responsible personnel provided reasonable assurance that actions were ongoing to develop operational contingency plans; however, the Federal Aviation Administration did not provide reasonable assurance that the Automated Radar Terminal/Tracking System will be Y2K compliant and fielded in a timely manner. In addition, the Army Aviation Center did not have any Y2K memorandums of agreement in place defining Y2K air traffic control responsibilities with the Federal Aviation Administration or the Air Force.

The memorandum recommended that the Commander, U.S. Army Aviation Center, prepare contingency plans for all air traffic control systems and that the Director, U.S. Army Aeronautics Services Agency, initiate communications with the Federal Aviation Administration and the Air Force to establish a memorandum of agreement/understanding, or amend existing maintenance agreements detailing Y2K responsibilities. Senior managers fully agreed with the recommendations and took immediate actions to resolve the risk issues identified during the assessment.

Memorandum Report No. AA 99-29, "Audit of Automated Information Systems – Year 2000 (Phase IV); Assessment of Selected Mission-Critical Systems at the Office of the Program Executive Officer for Command, Control, and Communications Systems," October 16, 1998. The report states that users of the Army Maneuver Control System are at moderate risk of potentially losing continuity of operations because of Y2K issues. The report discussed four risk areas relating to interfaces, test plans, contingency plans, and schedule slippage. Specifically, the report recommended that the Office of the Program Executive Officer, Command, Control, and Communications Systems:

- coordinate with interfacing system partners to ensure system interface agreements are prepared and signed for all interfacing systems no later than 1 October 1998.
- modify the test plan to incorporate the key testing information discussed in the Army's Year 2000 Action Plan.

- update the contingency plan to address key information outlined in the Army's year 2000 Action Plan.
- continue efforts to complete testing of the Maneuver Control System in time to meet the Army's Year 2000 guideline.

Program Executive Office representatives and the Product Manager for the Maneuver Control System fully agreed with the recommendations and developed planned actions to address each risk issue.

Memorandum Report No. AA 99-30, "Audit of Automated Information Systems – Year 2000 (Phase IV); Assessment of Selected Army Legacy Air Traffic Control Mission-Critical Systems," October 16, 1998. The report states that the U.S. Army Communications-Electronics Command established an effective Y2K oversight program and its senior managers were actively involved in overseeing Y2K remediation efforts. However, the report identified two high-risk issues requiring immediate attention. The Army Materiel Command used a simplified Y2K compliance certification checklist that did not ensure that system managers assessed critical areas such as embedded chips, microprocessors and interfaces. In addition, the Army Materiel Command did not report all its major subordinate commands' air traffic control systems to the Army's Y2K database.

The memorandum suggested that the Commander, U.S. Army Materiel Command:

- Issue command-wide guidance ensuring that the Army's Y2K Action Plan is adhered to.
- Comply with the Army's or the Command's Y2K Certification Checklist, and to discontinue use of less stringent Y2K certification checklist.
- Obtain General Officer or Senior Executive Service – HQDA Functional/System Proponent – certification authority for mission-critical systems.
- Forward completed certification checklists to HQDA.
- Report all mission-critical and major systems to the Army's Y2K database.

The Army Materiel Command agreed with all suggested actions and took immediate action to resolve the high-risk issues.

Inspector General, Navy

Report, "Visit to Chief of Naval Education and Training," January 15, 1999. The report states that the Chief of Naval Education and Training senior leadership is fully engaged and committed to ensuring that any Y2K problems encountered are minimal. However, the report discusses shortfalls in contingency plans, memorandum of agreements, and reporting. Specifically, the Chief of Naval

Education and Training prepared inadequate contingency plans and memorandums of agreement, and inaccurately reported system interfaces.

The report recommended that the Chief of Naval Education and Training continue with efforts to develop realistic and workable contingency and continuity of operations plans. The report also recommended that the Navy Y2K Project Office work with the System Commands to ensure that the Y2K status of training equipment is reported to the Chief of Naval Education and Training.

Y2K Assessment Point Paper, "Potential Loss of Operational Readiness and Confidence," December 18, 1998. The point paper states that representatives of Naval Fleet units expressed a loss of confidence in senior leadership's approach to Y2K issues. Battle Group front-line ships are concerned about the quantity and scope of Y2K changes, specifically, the rate of delivery of the changes and the lack of pierside technical support. It is widely believed that there are too few test engineers to oversee the testing of a large number of planned installations. In addition, while some integrated Y2K testing occurred, not all systems were scheduled to undergo integrated lab tests before their Y2K Battle Group Systems Integrated Tests. Further, the U.S.S. Constellation and the U.S.S. John F. Kennedy will be severely limited during the Battle Group Integrated Tests because implementation of Y2K fixes for combat and intelligence systems is not on schedule. The point paper recommended that the Naval Sea Systems Command:

- coordinate with other System Commands to promulgate all system upgrades through the Fleet Type Commands,
- continue to populate the newly established "A through O" database, and
- establish a management plan to detail how requirements of the Navy's Y2K Action Plan will be implemented for tactical systems.

Y2K Assessment Point Paper, "Facilities and Infrastructure Assessments," December 18, 1998. The point paper states that mission-critical inventories are largely complete but, as of December 7, 1998, only about 35 percent of the Navy's mission-critical facilities and infrastructure systems were assessed. In addition, claimants may be competing for limited Naval Air Warfare Center assessment resources. Because all claimants are proceeding independently with the facilities and infrastructure inventory and assessment, they are effectively competing for limited resources. The point paper recommended that the Naval Operations Command coordinate with claimants and the Naval Air Warfare Center to ensure that they consider Navywide priorities in assessing mission-critical facilities and infrastructure systems and pursue central funding to expedite or augment the Naval Air Warfare Center's assessment efforts.

Y2K Assessment Point Paper, "Communications/Information Technology Management Deficiencies," December 18, 1998. The point paper states that several recurring Y2K issues exist for communications and information technology infrastructure with Navy management. Specifically, the issues were

regionalization of communications and information technology management, lack of contingency plans, dependence on civilian infrastructure, and customer prioritization. The point paper recommended that:

- The Vice Chief of Naval Operations direct the acceleration of the regionalization of the N6 function throughout the Navy, including establishing clear administrative control over all regional telecommunications systems.
- Regional Commanders continue to develop contingency and continuity-of-operations plans.
- The Navy Computers and Telecommunications Command develop and promulgate infrastructure guidance for obtaining information from commercial telecommunications providers concerning possible service outages and risks associated with their Y2K problems.
- The Chief of Naval Operations coordinate with the Naval Fleets and regional commanders to prioritize customer telecommunications and network connections.

Y2K Assessment Point Paper, "Continuity of Naval Intelligence Operations and Theater Dependencies," December 18, 1998. The point paper states that Fleet intelligence managers are grappling with the problem of developing Y2K-related continuity of intelligence plans. The complexity of this task is compounded because:

- information required to develop intelligence continuity plans is inadequate,
- system contingency plans are generally not realistic, and
- national and theater intelligence managers did not develop contingency guidance.

The point paper recommended that intelligence theaters must provide a comprehensive perspective of the worst-case Y2K environment for national and theater architectures and systems. In addition, the point paper recommended that Joint Intelligence Centers:

- solicit realistic continuity-of-intelligence requirements from Component forces, and
- develop guidance in the form of a realistic continuity architecture based on Component requirements.

Y2K Assessment Point Paper, "Y2K Remediation Efforts for Foreign Military Sales," December 18, 1998. The point paper states that there is little effort underway to ensure that allies who have purchased U.S. equipment are aware of potential Y2K deficiencies. In addition, there is little evidence that U.S. allies are conducting integrated Y2K testing of U.S. military equipment.

As a result, allied or coalition efforts may be jeopardized in the event of a Y2K crisis. The point paper recommended that the International Program Office:

- examine the current policy of one-time Y2K notification to foreign military sales customers, and
- aggressively work with allied and NATO customers to identify potential integration problems of Y2K-remediated U.S. equipment.

In addition, the point paper recommended that the International Program Office and the Navy Systems Command develop a database to reflect the Y2K status.

Interim Report, "Visit to Commander in Chief, U.S. Atlantic Fleet," December 9, 1998. The report states that it is "extremely likely" that many U.S. Atlantic Fleet systems will not be Y2K compliant in time. The report discusses several major Y2K problems that may have a significant impact on the U.S. Atlantic Fleet. The most significant problem was the lack of progress being made by Atlantic Fleet units in identifying and addressing Y2K issues. The aircraft squadrons were mostly still in the assessment phase. In addition, the exact extent of renovation and implementation of required new hardware and software was largely unknown. The extent of the fixes required, once known, will likely have a significant impact on fleet schedules and workloads. The report recommended that the Commander in Chief, U.S. Atlantic Fleet, work closely with the system Commands to identify and schedule system renovations as soon as possible and disseminate the information to the unit level as soon as it is received.

Interim Report, "Visit to Commander in Chief, U.S. Naval Forces Europe," November 19, 1998. The report states that a significant number of the U.S. Naval Forces Europe systems will not be compliant by the year 2000. The report discusses the dependence of U.S. Naval Forces Europe on host-nation-supplied telecommunications systems for much of its critical operational and administrative needs. Specifically, the U.S. Naval Forces Europe intelligence activities are dependent on the Joint Worldwide Intelligence Communications System network for intelligence. The system depends on foreign commercial bandwidth and routing, which may not be Y2K compliant. Naval intelligence functions in Europe and Southwest Asia will be affected should Y2K-related infrastructure outages occur in host nations. The report recommended that the Commander in Chief, U.S. Naval Forces Europe, explore methods for reducing reliance on host-nation telecommunications systems.

Personnel resources are a major problem for the U.S. Naval Forces Europe because the level of personnel available to work Y2K issues is inadequate. The on-board manning of active duty personnel allows only 83 percent claimancy validated requirements. The report recommended that funding for reserve support be increased and dedicated to supporting Y2K issues.

Interim Report, "Visit to Commander in Chief, U.S. Pacific Fleet," November 5, 1998. The report states that the most significant problem was the lack of information available on Program of Record systems that affect Naval Fleet units. Of the hundreds of systems managed by Naval Sea and Air Systems Commands, almost no information provided to the U.S. Pacific Fleet Command or subordinate commands covered the potential Y2K impacts, scope of required

corrections, or contingency plans. Because of the lack of information, the U.S. Pacific Fleet Command is unable to schedule required system upgrades or prioritize funding. The report discusses the detrimental impact of not having the Naval Fleet fully compliant in time for the Navy's Battle Group Situation Y2K end-to-end tests scheduled for March 1999. The report recommended that the Naval Sea Systems Command and the Naval Air Systems Command provide timely information to the Naval Fleets on the current status of all Program of Record systems impacting fleet units.

The report also addresses space-borne reconnaissance systems that are not scheduled to achieve Y2K compliance until late summer or early fall 1999. The Navy's Battle Group Situation Y2K end-to-end tests will not be able to include space-borne reconnaissance systems if they are not compliant by March 1999.

Interim Report, "Visit to Chief of Naval Operations (N09B)," October 23, 1998. The report states that Chief of Naval Operations claimant activities will not implement all mission-critical programs by the required deadline. Many activities were still conducting assessment of facilities and infrastructure systems. The report states that without increased high-level management involvement from the Chief of Naval Operations and individual claimant activities, all mission-critical programs will not be compliant by the year 2000. The report recommended that the Chief of Naval Operations increase resources to manage Y2K issues, including hiring contractor support, and direct claimant activities to fully engage in managing Y2K issues, including developing reliable contingency and continuity-of-operations plans.

Actions Taken. The Department of the Navy, Chief Information Officer, provided an update to the Inspector General, Navy, reports. Some of the statements contained in the initial Inspector General, Navy, reports no longer reflect the current status of the Navy's efforts. As of February 26, 1999, the Navy stated that it:

- made all Battle Group Program of Record information available via websites at multiple echelon levels,
- began the U.S.S. Constellation Battle Group Systems Interoperability Testing Y2K exercise, and preparations continue for follow-on exercises, including end-to-end testing,
- completely renovated and certified 87.3 percent of Navy mission-critical Program of Record systems, which many will participate in the Unified Command Operational Evaluations this summer,
- inventoried 99.7 percent of the Navy Facilities and Infrastructure, and for most, implementation is well underway, and
- informed sailors of how the Navy is addressing Y2K on a systems level and how Y2K will affect them in their personal lives.

Naval Audit Service

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Research Laboratory, January 22, 1999. The memorandum states that the Naval Research Laboratory is on track to meet the DoD and Navy target completion dates. The Naval Research Laboratory was previously audited by the Inspector General, DoD, in May 1998, and the Naval Audit Service performed a follow-up review on the following five recommendations:

- develop a Y2K action plan,
- complete the inventory of all hardware, software, and firmware,
- develop test, contingency, and cost plans,
- review technology projects for Y2K impacts, and
- modify contracts to include the Federal Acquisition Regulation Y2K language.

The Naval Audit Service found that the Naval Research Laboratory had completed all recommendations.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Surface Warfare Center – Dahlgren Division, January 4, 1999. The memorandum states that the Naval Surface Warfare Center – Dahlgren Division will not meet the DoD or Navy Y2K target completion dates for any of the phases. In addition, the Naval Surface Warfare Center – Dahlgren Division did not develop continuity-of-operations or contingency plans. The memorandum recommended that the Naval Surface Warfare Center – Dahlgren Division update its contingency plans to include Y2K considerations, and develop and test continuity-of-operations plans for relief from possible Y2K failures.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Strategic Systems Programs, January 4, 1999. The memorandum states that the Strategic Systems Programs will not meet the DoD and Navy target completion dates for their mission support and infrastructure.

In addition, the Strategic Systems Programs did not:

- complete their infrastructure inventory as of November 19, 1998,
- complete their continuity-of-operations plan, and
- fully complete their contingency plans by providing for system operations while repairs to unexpected Y2K problems are corrected.

Further, the same contractors who designed, developed, maintained, and tested the systems on a regular basis were performing the level 1 system certifications. The memorandum recommended that the Strategic Systems Programs update all contingency plans, complete continuity-of-operations plans, and ensure that

level 1 certifications are performed by independent testing contractor personnel who are not involved in the normal day-to-day design, development, maintenance, and testing of the systems.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Sea Command's SEA-08 Nuclear Propulsion, January 4, 1999. The memorandum states that the SEA-08 is on track to meet the DoD and Navy target completion dates. The SEA-08 has contingency plans in place, interface agreements signed, and all phases for infrastructure items finished. The report made recommendations addressing minor database issues.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Bureau of Medicine and Surgery, December 23, 1998. The memorandum states that the Bureau of Medicine and Surgery is at risk of not meeting DoD and Navy Y2K target completion dates. In addition, the Bureau of Medicine and Surgery did not complete the inventory for Infrastructure Productivity Devices and did not identify all infrastructure items for internal Y2K tracking. Further, the Bureau of Medicine and Surgery tracks a unique category for infrastructure items and biomedical devices, which is not a standard infrastructure category as defined by the Navy Y2K Action Plan. The report recommended that the Chief Information Officer for the Navy provide guidance to the Bureau of Medicine and Surgery for tracking and reporting the unique category of biomedical devices.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Military Sealift Command, November 12, 1998. The memorandum states that the Military Sealift Command will not meet the DoD and the Department of the Navy's Y2K target completion dates. The report discusses several high-risk areas that require the Military Sealift Command's immediate attention including contingency and continuity of operations plans, contract language, and reporting. The Military Sealift Command did not sign or test their contingency plans, and did not develop a continuity-of-operations plan as required by Navy guidance. In addition, contracts did not contain appropriate Y2K language as required by Federal Acquisition Regulation 39.002. Further, the Military Sealift Command did not accurately report their systems in the Navy's Y2K database. The memorandum made several recommendations relating to the risk areas mentioned above.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Norfolk Naval Shipyard, November 9, 1998. The memorandum states that the Naval Sea Systems Headquarters did not provide Y2K guidance to the Norfolk Naval Shipyard in a timely and consistent manner; consequently, the shipyard will not meet its target completion dates for any of the Y2K phases. The report discusses several risk areas that require the shipyard's immediate attention, including continuity-of-operations and contingency plans, and contract language. The memorandum recommended that the Norfolk Naval Shipyard update their continuity-of-operations plans, develop contingency plans for all corporate systems, and revise Y2K contract language to include Federal Acquisition Regulation 39.002.

The Naval Audit Service is to conduct another review of the Norfolk Naval Shipyard when it reviews the Portsmouth Naval Shipyard. The memorandum did not state when the follow-up review would commence.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Sea Systems Command Headquarters, October 28, 1998. The memorandum states that the Naval Sea Systems Command did not:

- develop continuity-of-operations plans,
- complete Y2K certification checklists,
- maintain adequate Y2K documentation to show how problems were identified and corrected, and
- accurately report systems in the Navy Y2K database.

The memorandum recommended that the Naval Sea Systems prioritize resources to ensure that contingency plans, testing, and required Y2K documentation meet the DoD and Navy's target completion dates.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Air Systems Command, October 22, 1998. The memorandum states that the Naval Air Systems Command did not accurately report systems in the Navy Y2K database. For example, the System for Analysis of Financial Resources and the Budget Execution System were being reported in the implementation phase, even though interface agreements were not signed. The memorandum suggested that Naval Air Systems Command commit additional resources to develop contingency plans and ensure that system interface memorandum of agreements are in place.

Air Force Audit Agency

Briefing Report, "Continuity of Mission and Support Functions for the Year 2000 Program," October 9, 1998. The briefing report states that major Command installations were behind schedule in achieving milestones for the Y2K infrastructure program. Specifically, of the 49 installations reviewed:

- 45 needed to improve their efforts to complete inventory phase requirements,
- 44 needed to improve their assessment efforts, and
- 47 needed to improve or initiate implementation actions.

The inventory phase required that the major Command installations complete the infrastructure inventory, identify all mission-critical items, and assign appropriate criticality levels. The overall assessment efforts required a completed risk assessment, cost estimates, continuity-of-operations plans, and support and coordination with critical vendors. The implementation actions required

corrective actions on assessed items, initiating contingency or continuity-of-operations plans, planning for crisis response teams, and developing testing and exercise scenarios. The briefing report recommended:

- establishing weekly installation status briefings,
- improving coordination between major Commands and installation focal points,
- improving the distribution process for Y2K guidance,
- improving working group effectiveness,
- establishing, monitoring, and enforcing an installation schedule to support Air Force and major Command milestones, and
- performing random reviews of critical items to validate actions planned or taken, and coordinating and scheduling joint exercises among installation units.

Appendix C. Year 2000 Memorandums

The Under Secretary of Defense (Comptroller) and the Senior Civilian Official have recently issued additional guidance for DoD Y2K efforts.

Emergency Funding. On November 10, 1998, the Under Secretary of Defense (Comptroller) issued the memorandum, "The Fiscal Year (FY) 1999 Emergency Supplemental Appropriation for Information Technology Systems and Security Funds," to the Senior Civilian Official, Office of the Assistant Secretary of Defense. The memorandum states that the FY 1999 Omnibus Appropriations Bill contains $1.1 billion for emergency expenses relating to Y2K conversion efforts. In developing the Y2K emergency funding plan, the Senior Civilian Official should include the following:

- the requirement for critical infrastructure protection ($70 million),
- the immediate need to procure Y2K-compliant switches ($142 million), and
- the intent that reductions to automatic data processing legacy systems' operations and maintenance be shifted to meet Y2K compliance requirements ($298 million).

The Senior Civilian Official is responsible for determining the priorities for the balance of the $1.1 billion in emergency funds needed for Y2K compliance requirements.

Database Reporting, Interface Agreements, and Contracts. On September 23, 1998, the Senior Civilian Official issued the memorandum "Year 2000 (Y2K) Compliance – FY 1999 Reporting Requirements." The memorandum provides Y2K guidance for database reporting, interface agreements, and contract requirements. The memorandum states that the Military Departments, the Commanders-in-Chief, and Defense agencies are responsible for consistent, accurate, and timely submissions for the DoD Y2K database, and that each Component must ensure compliance with the memorandum, "Year 2000 Database Reporting," dated June 19, 1998.

Funding Requirements. On behalf of the Deputy Secretary of Defense, the Senior Civilian Official responded to the Office of Management and Budget Memorandum M-98-14, "Comprehensive Plans and Associated Funding Requirements for Achieving Year 2000 Computer Compliance," by stating that DoD:

- does not anticipate requiring additional FY 1999 funding for Y2K computer compliance costs,
- will fund all currently known FY 1999 Y2K efforts from the FY 1999 budgets, and

- will address Y2K as a national security issue and resource Y2K conversion efforts accordingly.

DoD will conduct military Y2K operational evaluations and end-to-end tests of its mission-support capabilities to verify operational readiness.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
- Deputy Under Secretary of Defense (Environmental Security)
- Deputy Under Secretary of Defense (Industrial Affairs and Installations)
- Deputy Under Secretary of Defense (Logistics)
- Director, Defense Procurement
- Director, Defense Research and Engineering
- Director, Defense Logistics Studies Information Exchange
- Director, Strategic and Tactical Systems
- Director, Test Systems Engineering and Evaluation
- Assistant to the Secretary of Defense (Nuclear, Chemical, and Biological Defense Programs)
- Defense Science Board

Under Secretary of Defense for Policy
Under Secretary of Defense (Comptroller)
- Deputy Chief Financial Officer
- Deputy Comptroller (Program/Budget)
- Director, Program Analysis and Evaluation

Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Health Affairs)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
- Deputy Assistant Secretary of Defense (Command, Control, Communications, Intelligence, Surveillance, Reconnaissance, and Space Systems)
- Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
- Principal Director for Year 2000

Assistant Secretary of Defense (Legislative Affairs)
Assistant Secretary of Defense (Public Affairs)
Director, Operational Test and Evaluation

Joint Staff

Director, Joint Staff

Department of the Army

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

Department of the Navy

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

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer, Department of the Air Force
Inspector General, Department of the Air Force
Auditor General, Department of the 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, Ballistic Missile Defense Organization
  Chief Information Officer, Ballistic Missile Defense Organization
Director, Defense Advanced Research Projects Agency
  Chief Information Officer, Defense Advanced Research Projects Agency
Director, Defense Commissary Agency
  Chief Information Officer, Defense Commissary Agency
Director, Defense Contract Audit Agency
  Chief Information Officer, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
  Chief Information Officer, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Legal Services Agency
  Chief Information Officer, Defense Legal Services Agency

Other Defense Organizations (cont'd)

Director, Defense Logistics Agency
  Chief Information Officer, Defense Logistics Agency
Director, Defense Security Assistance Agency
  Chief Information Officer, Defense Security Assistance Agency
Director, Defense Security Service
  Chief Information Officer, Defense Security Service
Director, Defense Threat Reduction Agency
  Chief Information Officer, Defense Threat Reduction Agency
Director, National Security Agency
  Inspector General, National Security Agency
Director, Washington Headquarters Services
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
  Office of Information and Regulatory Affairs
General Accounting Office
  National Security and International Affairs Division
    Technical Information Center
  Director, Defense Information and Financial Management Systems, Accounting and Information Management Division

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

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

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments

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

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

25 MAR 1999

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT
DIRECTORATE, INSPECTOR GENERAL, DoD

SUBJECT: Summary of DoD Year 2000 Audit and Inspection Reports II
(Project No. 8AS-0032.22)

This office has reviewed the Draft Audit Report on the Summary of DoD Year 2000 Audit and Inspection Reports II, dated March 10, 1999.

It is recommended that the report address the differences between system contingency and operational contingency plans. This could be done by modifying the matrix on pages five and seven to reflect DoD guidelines for both system and operational contingency plans during the audit timeframe. My experts request continued emphasis on contingency plans and believe your actions will result in greater awareness of the need for solid and effective operational contingency plans.

Please be advised that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) web site address for contingency planners (page eight of the draft report) has changed. The new address is:

http://www.c3i.osd.mil/org/cio/y2k/y2k_con_plan/index.html.

As you know, we are now into the testing cycle of our mission critical systems. Appendix I of our management plan (Testing Management Requirements) is approved and on the web We have met with members of your office, GAO, and the Services. Our Y2K Testing Directorate continues to focus on JS/CINC Y2K Operational Evaluations; Functional Area Y2K End-to-End Tests; Service-sponsored Y2K System Integration Tests; and Megacenters.

I want to personally thank everyone in the DoD Inspector General's Office for the hard work they have done providing oversight on the Year 2000 project. We have come a long way but we are not there just yet. Please stay on it as we get closer to the event horizon.

William A. Curtis
Principal Director, Year 2000

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
James W. Hutchinson
Timothy J. Harris
John J. Jenkins
Maria R. Palladino