Audit Report

SUMMARY OF DOD YEAR 2000 CONVERSION--AUDIT AND INSPECTION RESULTS

Report No. 99-059 December 24, 1998

Office of the Inspector General
Department of Defense

Additional Copies

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

Suggestions for Future Audits

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

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

Defense Hotline

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

Acronym

Y2K	Year 2000

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

December 24, 1998

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

SUBJECT: Report on Summary of DoD Year 2000 Conversion--Audit and Inspection Results (Report No. 99-059)

We are providing this report for information and use. Because this report contains no new findings or recommendations, no written comments were required, and none were received.

Questions on the audit should be directed to Mr. Scott S. Brittingham at (703) 604-9068 (DSN 664-9068) or Ms. Mary Lu Ugone at (703) 604-9049 (DSN 664-9049). 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. 99-059 **December 24, 1998**
(Project No. 8AS-0032.12)

Summary of DoD Year 2000 Conversion--Audit and Inspection Results

Executive Summary

Introduction. This report summarizes 142* audit and inspection reports, reviews, and memorandums pertaining to DoD organizations or functions and their year 2000 conversion progress. The reports were issued from August 1997 to December 1998.

Objective. The objective of this report is to summarize Y2K issues identified in General Accounting Office; Inspector General, DoD; Army; Navy; and Air Force audit reports from August 1997 to December 1998. We also included information reported by the Inspector General, Navy, and the Inspector General, Marine Corps. The Inspector General, Army, and the Inspector General, Air Force, had not yet reported on Y2K.

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

- management oversight and awareness (95 reports),
- reporting (79 reports),
- assessment (97 reports),
- resource requirements estimation (48 reports),
- interface identification and agreements (74 reports),
- prioritization (14 reports),
- testing (83 reports),
- contingency and continuity-of-operations planning (105 reports),
- contracts (21 reports), and
- infrastructure (44 reports).

The results support the DoD acknowledgements that the year 2000 conversion poses a high risk for a very wide range of DoD functions and organizations and that the conversion progress to date has been insufficient. Continued extensive audit and inspection coverage is planned.

---

*The 142 includes 3 Air Force Audit Agency summary reports that summarize a total of 61 Air Force Audit Agency installation reports.

Management Comments. We provided a draft of this report on November 12, 1998. Because this report contains no findings or recommendations, written comments were not required, and none were received. Therefore, we are publishing this report in final form.

Table of Contents

Executive Summary

Introduction

Background 1
Objective 3

Finding

Year 2000 Challenges 4

Appendixes

A. Matrix of Year 2000 Issues 10
B. Synopsis of Year 2000 Issues 18
C. Air Force Audit Agency Installation Reports 102
D. Report Distribution 107

Background

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

Because of the potential failure of computers to run or function throughout the Government, the President issued an Executive Order, "Year 2000 Conversion," February 4, 1998, making it policy that Federal agencies ensure that no critical Federal program experiences disruption because of the Y2K problem. The Executive Order also requires that the head of each agency ensure that efforts to address the Y2K problem receive the highest priority attention in the agency.

DoD Y2K Management Strategy. In his role as the DoD Chief Information Officer, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued the "DoD Year 2000 Management Plan" (DoD Management Plan) in April 1997. The DoD Management Plan provides the overall DoD strategy and guidance for inventorying, prioritizing, fixing, or retiring systems, and monitoring progress. The DoD Management Plan states that the DoD Chief Information Officer has overall responsibility for overseeing the DoD solution to the Y2K problem. In October 1998, the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) reorganized and expanded its Y2K organization. The Principal Deputy-Y2K, reports to the Deputy Chief Information Officer. The Deputy Chief Information Officer is responsible for Chief Information Officer policy and implementation.

Also, the DoD Management Plan makes the DoD Components responsible for implementing the five-phase Y2K management process. The "DoD Year 2000 Management Plan, For Signature Draft Version 2.0" (Draft DoD Management Plan), June 1998, accelerated the target completion dates for the renovation, validation, and implementation phases. The new target completion date for implementation of mission-critical systems is December 31, 1998, and for non-mission-critical systems is March 31, 1999. The release of the final plan was still pending as of December 17, 1998.

The DoD implementation goal for mission-critical systems is slightly more aggressive than the overall Federal Government implementation target. In a memorandum dated January 20, 1998, for the heads of executive departments and agencies, the Office of Management and Budget established a target date of March 1999 for implementing corrective actions to all systems.

Office of the Secretary of Defense Memorandums. The Secretary of Defense and the Deputy Secretary of Defense have issued significant guidance for DoD Y2K efforts.

Y2K Compliance. The Secretary of Defense issued the memorandum "Year 2000 Compliance" on August 7, 1998, which asserted that DoD was making insufficient progress on Y2K conversion. He directed a number of actions, including the following:

- The Joint Chiefs of Staff were to develop a Joint Y2K operational evaluation program and provide the plans to the Secretary of Defense by October 1, 1998.

- The Unified Commanders-in-Chief were to review the status of Y2K implementation within their command and the command of subordinate components.

- The Senior Readiness Oversight Council was to report the readiness implications of Y2K.

- The Services and Defense agencies were to report every Acquisition Category I, IA, and II system within their purview. The report was to address Y2K compliance or areas of noncompliance of each respective system.

- The Defense Information Systems Agency was to provide a report to the Office of the Secretary of Defense (Command, Control, Communications, and Intelligence) by October 15, 1998, listing all megacenter domain users who failed to sign explicit agreements with the Defense Information Systems Agency by October 1, 1998. Based on the Office of the Secretary of Defense (Command, Control, Communications, and Intelligence) recommendations, the Office of the Under Secretary of Defense (Comptroller) was to withhold domain users funds.

- The Office of the Under Secretary of Defense (Comptroller) was to issue guidance to the Military Departments and Defense agencies on the funding prohibitions before October 1, 1998.

Additionally, the Secretary of Defense directed that the Military Departments, Commanders-in-Chief, and Defense agencies ensure that the following takes place effective October 1, 1998:

- the list of mission-critical systems under their respective purview be accurately reported in the DoD Y2K database, with each change in mission-critical designation reported and explained to the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) within 1 month of the change;

- funds are not obligated for any mission-critical system in the Y2K database that lacks a complete set of formal interface agreements for Y2K compliance;

- funds are not obligated for any information technology or national security system contract that processes date-related information and that does not contain the Y2K requirements specified in Federal Acquisition Regulation 39.106, "Year 2000 Compliance"; and

- funds are not obligated for any domain user in a Defense Information Systems Agency Megacenter if that domain user failed to sign all associated explicit test agreements with the Defense Information Systems Agency.

Y2K Verification. The Deputy Secretary of Defense issued a memorandum "Year 2000 (Y2K) Verification of National Security Capabilities" on August 24, 1998. The memorandum states that the Chief of Staff of the Army, the Chief of Naval Operations, the Chief of Staff of the Air Force, the Commandant of the Marine Corps, and the Directors of the Defense Agencies must certify that they have tested the Y2K capabilities of their respective component's information technology and national security systems in accordance with the DoD Management Plan. In addition, all Principal Staff Assistants of the Office of the Secretary of Defense were to verify that all functions under their purview will continue unaffected by Y2K issues. Each Principal Staff Assistant was required to provide the Deputy Secretary of Defense with plans for Y2K-related, end-to-end testing of each process within the areas of logistics, personnel, health and medical, communications, and intelligence. Each Principal Staff Assistant was to certify that the test plan includes the following:

- functional risk assessments,
- Y2K effects on continuity-of-business operations, and
- associated contingency plans.

Further, the test plans were to include all mission-critical systems involved in each test. The Director, Operational Test and Evaluation, was to help the Principal Staff Assistants with cross-functional, inter-Service, and cross-system testing.

Objective

The objective of this report is to summarize Y2K issues identified in General Accounting Office; Inspector General, DoD; Army; Navy; and Air Force audit reports from August 1997 to December 1998. We also included information reported by the Inspector General, Navy, and the Inspector General, Marine Corps. The Inspector General, Army, and the Inspector General, Air Force, had not yet reported on Y2K. Appendix A provides a matrix of issues identified in the 142* reports, memorandums, and reviews that involved DoD organizations. Appendix B contains a summary of the problems identified and corrective actions recommended in each publication listed in the matrix.

*The 142 includes 3 Air Force Audit Agency summary reports that summarize a total of 61 Air Force Audit Agency installation reports.

Year 2000 Challenges

Management Oversight and Awareness. Leadership focus is the key in awareness. DoD Components should have promoted Y2K awareness vigorously across organizations and at all levels of leadership. DoD Components must prepare the necessary plans and must focus and prioritize their organizational missions to attack the Y2K problem. However, to perform, DoD Components must first understand the size, pervasiveness, and scope of the Y2K problem. All participants in the Y2K process must understand the need to collect and disseminate information on lessons learned and best practices. The President's Council on Year 2000 Conversion assigned sectors of the Federal Government, such as defense, telecommunications, and education, to lead Federal agencies who coordinate, plan, and direct Y2K actions for all other agencies. Areas of interest assigned to DoD as the lead Federal agency include the following:

- Defense industry,
- Defense treaties and alliances,
- Military treaty obligations, and
- Defense coalitions and mutual support agreements.

The need for improved management oversight and awareness is discussed in 95 reports. Recommendations for improvement were made to a very wide range of DoD Components, including the Office of the Secretary of Defense, the Joint Staff, Unified Commands, Military Department Headquarters, Defense agencies, major commands, and individual units. The range of components included the following: the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence); U.S. Pacific Command; U.S. Atlantic Command; Army Deputy Chiefs of Staff for such areas as Installation Management, Intelligence, and Logistics; the Army Reserve Command; the Naval Air Systems Command; the Naval Sea Systems Command; the Naval Research Laboratory; the Air Combat Command; the Air Force Standard Systems Group; the 552nd Air Control Wing; and the Defense Information Systems Agency.

Reporting. The Office of Management and Budget requires DoD to submit a quarterly Y2K report. The report provides a status of DoD Y2K compliance efforts and provides progress information to the Executive Branch, Congress, and the public. DoD Components are required to submit Y2K status information to the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), which submits the Y2K status report to the Office of Management and Budget.

The Draft DoD Management Plan states that DoD Components are required to manage and maintain a database that provides a composite picture of DoD Y2K information. Further, the DoD Components are required to forward system information to a DoD centralized database, which serves as the repository for the Office of the Secretary Defense and provides summary-level data. The repository is used to report to Congress and the Office of Management and Budget, as required. Appendix I of the Draft DoD Management Plan describes the Y2K

reporting requirement. The process is designed to accomplish Y2K reporting without additional data calls to the DoD Components. If the process is implemented properly, it will meet the Y2K reporting requirements levied by Congress, the Office of Management and Budget, and DoD.

Problems associated with reporting are discussed in 79 reports. For example, Inspector General, DoD, Report No. 98-077, "Year 2000 Computing Problem Reports: August 1997 Report," February 18, 1998, states that DoD Components' second-quarter reports on the Y2K issue were incomplete and unreliable. Additionally, DoD Components inconsistently interpreted the Chief Information Officer's reporting requirements. Also, DoD did not establish clear reporting guidance and requirements. As a result, DoD was not able to effectively measure its Y2K progress. In November 1998, the Inspector General, DoD, commenced a followup audit that would evaluate whether DoD made progress in improving its reporting.

Assessment. The assessment process includes an inventory of all systems, identifies mission-critical systems with an evaluation of each system's Y2K risks and issues, develops a strategy to address each risk, prioritizes all systems for fixing, and develops contingency plans. The assessment phase tasks are to define the size and the scope of the Y2K problem, decide on the appropriate strategy to resolve it, and identify the plan needed to assign the resources that would yield a compliant system.

Problems associated with the assessment phase are discussed in 97 reports. The reports are addressed to a very wide range of DoD Components, including Unified Commands, Military Department Headquarters, Defense agencies, major commands, and individual units. The range of components included the U.S. Transportation Command, the Army National Guard, the Ballistic Missile Defense Organization, the Space and Naval Warfare Systems Command, the Naval Strike and Air Warfare Center, and the Air Force Materiel Command.

Resource Requirements Estimation. For DoD Components to effectively prioritize and allocate resources, they need to estimate the monetary and personnel costs to find, fix, and test Y2K-noncompliant systems. Additionally, DoD Components should accumulate Y2K-related cost data, as well as personnel and equipment requirements, so that they may reasonably assess the magnitude of the Y2K problem and accurately identify critical budget shortfalls.

The need for more accurate resource requirements estimation is discussed in 48 reports. The reports are addressed to various DoD components, including the Army, the Navy, the Air Force, the Defense Finance and Accounting Service, and the Defense Information Systems Agency. For example, reports on the following DoD Major Ranges and Test Facilities: Army Kwajalein Missile Range, Navy Pacific Missile Range Facility, and Nellis Air Force Base identified a need for better cost estimation and the impact that poor cost estimation could have on the budget. The reports illustrate that DoD resource requirements estimates were understated but that the amount of understatement was unknown.

Interface Identification and Agreements. Interfaces are critical to the Y2K effort because they have the potential to propagate errors from one system, organization, or function to another. Therefore, DoD system owners need to identify system data exchange interfaces and document agreements with other

system owners on data exchange format and protocols. The Draft DoD Management Plan provides a sample agreement that is required for interfaces external to DoD and among DoD Components.

The need for better interface identification and agreements is discussed in 74 reports. For example, Air Force Audit Agency Project No. 97066036, "Systems Assessment for the Year 2000 Program," May 21, 1998, states that Air Force activities did not properly evaluate system interfaces during the assessment process because activities did not dedicate the necessary resources to effectively progress beyond identifying systems; system managers often considered coordinating interfaces the sole responsibility of the activity receiving their data and, therefore, did not initiate contact; and some activities planned to postpone identifying interfaces until after initiating system renovations, even though such procedures could result in costly reworks.

Prioritization. The DoD Management Plan states that systems that are critical to the support of the DoD warfighting and peacekeeping mission and those that affect the safety of individuals should receive priority for conversion and replacement. DoD Components must prioritize their mission-critical systems to determine which systems should be remediated first. Further, DoD Components should assess the mission impact of a system's or interface's failure to determine the system that should receive the highest priority. System prioritization is essential so that components can determine the relative merits of fixing one system instead of another in case DoD Components cannot reallocate enough resources or skilled personnel to fix all systems in time.

The need for prioritization is discussed in 14 reports. For example, General Accounting Office Report No. AIMD-98-72 (OSD Case No. 1562), "Defense Computers: Year 2000 Computer Problems Threaten DoD Operations and National Security," April 30, 1998, states that DoD Components' system prioritization for correction was one of the systemic weaknesses of the Y2K programs. The report states that DoD needed to decide the relative priority of its mission-critical systems and ensure that mission-critical, rather than non-mission-critical, systems receive focused management attention and resources. However, according to DoD status reports, DoD was correcting non-mission-critical systems nearly as quickly as its mission-critical systems.

Testing. The Draft DoD Management Plan requires the following three levels of testing:

- Individual system renovation and certification testing is generally performed by the developer or owner of the software, and all mission-critical systems are required to be renovated, certified, and implemented by December 31, 1998.

- Functional-centric testing describes tests that are specifically developed to validate Y2K compliance. The tests are performed on multi-system interfaces to ensure that individual Y2K-compliant systems correctly interface with other systems.

- Mission-centric testing evaluates the ability of Y2K-compliant, mission-critical systems to operate with other systems in support of the operational mission.

The Draft DoD Management Plan requires that system developers and maintainers, as well as the system's functional proponent, certify and document each system's Y2K compliance. System certification requires the system manager, the project manager, and the customer to sign the compliance checklist confirming that testing was completed in accordance with the Draft DoD Management Plan.

Testing-related issues are discussed in 83 reports. For example, Air Force Audit Agency Project No. 98066019, "Management Advisory Service, Phase Status Validation for the Year 2000 Program," June 10, 1998, states that system managers did not support test conclusions for 34 of 86 systems reported as in the implementation phase or completed. Additionally, Inspector General, DoD, Report No. 98-147, "Year 2000 Certification of Mission-Critical DoD Information Technology Systems," June 5, 1998, states that DoD Components were not complying with Y2K certification criteria before reporting systems as Y2K compliant. The report estimates that DoD Components certified only 109 (25.3 percent) of the 430 systems reported as Y2K compliant.

Contingency and Continuity-of-Operations Planning. Contingency and continuity-of-operations planning is required to lessen the threat of Y2K failures and to ensure that those essential functions continue to operate. No guarantee exits that all DoD systems will be fully renovated and risk-free by January 1, 2000. Further, renovated and tested systems could fail, and the failure of one system could disrupt many others. Therefore, contingency and continuity-of-operations planning is a critical responsibility of DoD Components. The Draft DoD Management plan states that although system managers are responsible for system contingency planning, DoD Components (users) are responsible for developing a component continuity-of-operations plan. Contingency and continuity-of-operations planning shortfalls are discussed in 105 reports.

Contingency Planning. Contingency planning addresses known or suspected sources of disruption and unanticipated disruptions. Specifically, contingency plans address:

- failures of systems believed to be Y2K compliant,
- failures of interfaces,
- transfers of corrupt data, and
- failures of utilities or other infrastructure elements necessary for operation, or
- any other items that could result in a Y2K-related failure.

The General Accounting Office Report No. AIMD-98-85, "Year 2000 Computer Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships," April 30, 1998, states that time is rapidly winding down for the Federal Government to set priorities to focus Y2K efforts on the most important systems and to ensure that the systems receive appropriate testing. As a result,

any uncertainties regarding Y2K compliance for agencies' internal systems, systems of the data partners, and systems that support the public infrastructure make developing and testing contingency plans an essential task.

Continuity-of-Operations Planning. Continuity-of-operations planning is the process of identifying, assessing, managing, and mitigating Y2K risks to ensure continuity of core business processes. The General Accounting Office publication, "Year 2000 Computing Crisis: Business Continuity and Contingency Planning," August 1998, states that Federal agencies should not limit risk reduction planning to the risks posed by the Y2K-induced failures of internal information systems. Federal agencies must include the potential Y2K failures of others, including business partners and infrastructure service providers. The Draft DoD Management Plan states that the continuity-of-operations plan should include a list of DoD Component systems and major actions taken to minimize Y2K disruption, which would be useful in prioritizing response sequence and resource use in the event of widespread disruptions.

The need for better DoD continuity-of-operations planning is discussed in 45 reports. The reports are addressed to various DoD Components, including the Navy; the U.S. European Command; the U.S. Southern Command; the Army Reserve Command; and the Defense Information Systems Agency. For example, the General Accounting Office Report No. AIMD-98-150 (OSD Case No. 1622), "Defense Computers Year 2000 Computer Problems Put Navy Operations at Risk," June 30, 1998, states that the Navy was not developing contingency plans that focused on ensuring the continuity of all of its critical military operations and business processes. Instead, the Navy was developing plans for only a small portion of its mission-critical systems. Based on the Navy criteria, it would have developed contingency plans for only 7 of its 812 mission-critical systems.

Contracts. The Federal Acquisition Regulation 39.002, "Definitions," states that information technology is Y2K compliant when it is capable of accurately processing date and time data (such as calculation, comparing, and sequencing) in both the twentieth and twenty-first centuries as well as in leap years. The Federal Acquisition Regulation 39.106, "Year 2000 Compliance," states that agencies acquiring information technology that requires date and time processing after December 31, 1999, must ensure that contracts and solicitations require Y2K compliance. It also states that agencies must ensure that noncompliant information technology is upgraded to be Y2K compliant.

Failure to follow guidance when contracting for Y2K-compliant products is discussed in 21 reports. For example, Inspector General, DoD, Report No. 98-207, "Year 2000 Contract Language for Weapon Systems," September 22, 1998, states that of the 16 weapon systems reviewed, 9 systems had contracts that did not contain language from Federal Acquisition Regulation 39.106, "Year 2000 Compliance." The Under Secretary of Defense for Acquisition and Technology initially had not issued Y2K guidance for weapon systems. However, on August 7, 1998, the Secretary of Defense directed the Services and Defense agencies to report on each major acquisition system under their purview. Each report should address areas of Y2K compliance or noncompliance for each system. The Secretary of Defense also directed that funds not be obligated for any contract for information technology or national security systems that process date-related information and that does not contain Y2K requirements specified in Section 39.106 of the Federal Acquisition Regulation.

Infrastructure. The computer and communication hardware, software, databases, people, facilities, and policies supporting an enterprise's information management functions are considered infrastructure. The Draft DoD Management Plan defines policies for inventory and reporting devices controlled by information technology and used in the infrastructure of DoD installations. Devices controlled by information technology are subject to Y2K vulnerabilities and may include traffic control systems, water and sewage treatment systems, security systems, and telephone switches. Infrastructure as a high-risk Y2K issue is discussed in 44 reports. The reports are addressed to various DoD Components including the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence); the Naval Air Systems Command; the Naval Sea Systems Command; and medical facilities such as Reynolds Army Community Hospital.

Conclusion

The results of the extensive audit and inspection coverage discussed in this report support the Secretary of Defense assessment that high risk exists and the DoD progress in meeting the year 2000 conversion challenge has been insufficient. All major DoD Components--the Office of the Secretary of Defense, the Joint Staff, Military Departments, Defense agencies, and Unified Commands--must intensify their efforts in the limited time left before the new millenium. We anticipate continued involvement by the audit and inspection community on a very large scale as the conversion effort continues.

Appendix A. Matrix of Year 2000 Issues

Report No.	Organization/ Function	Ap.B Page	Over.& Awar.	Report.	Assess.	Resour. Est.	Interf.	Priorit.	Testing	Cont.& Coop.	Ctracts.	Infrast.
General Accounting Office												
AIMD-98-124	Electronic Data Exchanges	18					X					
AIMD-98-150	Navy	18	X	X	X	X	X		X	X		
AIMD-98-53	Army	19	X	X	X	X	X		X	X		
AIMD-98-85	DoD	20	X	X	X	X	X	X	X	X		
AIMD-98-72	DoD	21	X	X	X	X	X	X	X	X		
AIMD-98-35	Air Force	22		X	X	X	X		X	X		
AIMD-98-7R	Naval Supply Systems Command	23					X			X		
AIMD-97-149	Logistics Systems Support Center	23					X	X	X	X		
AIMD-97-120R	Standard Systems Group	24	X				X					
AIMD-97-112	DIST database	24		X	X							
AIMD-97-106	Defense Logistics Agency	25	X		X		X	X		X		
AIMD-97-117	Defense Finance and Accounting Service	25	X				X		X	X		
Inspector General, DoD												
99-058	Defense Critical Suppliers	26			X							
99-055	DoD Health Care	26	X	X	X		X		X	X	X	X
99-052	Logistics and Maintenance /AWACS	27	X	X			X		X	X		
99-049	Defense Finance and Accounting Service	27				X				X		
99-046	Army Kwajalein Missile Range	29		X	X	X		X	X	X		
99-039	552nd Air Control Wing	29	X	X	X			X	X	X		X
99-038	Pacific Missile Range Facility	30		X	X	X						

Report No.	Organization/ Function	Ap.B Page	Over.& Awar.	Report.	Assess.	Resour. Est.	Interf.	Priorit.	Testing	Cont.& Coop.	Ctracts.	Infrast.
99-036	Army Research Laboratory	30	X		X		X				X	X
99-035	AMR Institute of Infectious Diseases	31	X	X	X	X			X	X	X	X
99-034	On-Site Inspection Agency	31	X						X	X		
99-031	U.S. Pacific Command	32	X	X	X				X	X		X
99-030	Defense Technology Security Admin.	33	X	X					X	X		
99-028	Defense Special Weapons Agency	34	X	X					X	X		
99-027	DoD Base Comm. Systems	34								X		X
99-022	Army Major Ranges and Test Facilities	35										
99-017	Airborne Warning and Control System	35								X	X	
99-015	JBC, JC2WC, JCSE, JWAC, JWFC	36			X				X	X		
99-003	Air Force Research Laboratory	36			X						X	X
98-218	Naval Air Warfare Center	36	X	X	X							
98-203	Naval Research Laboratory	37	X		X	X			X	X	X	
98-207	Y2K Ctract Language-Weapon Systems	38									X	
98-196	Navy SAP Program Community	38										
98-194	U.S. Atlantic Command	38	X	X	X				X	X		
98-193	Defense Information Systems Agency	39		X					X	X		
98-188	U.S. Space Command	41	X		X		X		X	X		
98-187	AF Major Range and Test Facilities	42	X		X	X						
98-184	Defense Information Systems Agency	43	X	X		X	X	X	X	X		
98-182	DARPA	44									X	
98-180	BMDO	44	X	X	X						X	
98-173	U.S.Central Command	45	X		X		X		X	X		

Report No.	Organization/ Function	Ap.B Page	Over.& Awar.	Report.	Assess.	Resour. Est.	Interf.	Priorit.	Testing	Cont.& Coop.	Ctracts.	Infrast.
98-169	Lessons learned from DIST database	46	X	X								
98-147	Y2K certification	47	X	X					X			
98-129	U.S. Special Operations Command	48	X	X	X	X	X		X	X		
98-112	Defense Finance and Accounting Service	49		X								
98-111	Defense Finance and Accounting Service	49		X	X		X		X			
98-077	DoD August 1997 report	51	X	X								
98-074	Sharing Y2K testing information	51	X						X			
98-068	Air Force SAP	52			X				X			
98-065	DoD IT solicitations and contract compliance	52	X								X	
Army Audit Agency												
AA 98-350	Raymond W. Bliss Army Health Center	53	X		X	X		X	X	X		X
AA 98-313	Special Access Programs	53		X	X		X			X	X	
AA 98-201	Special Access Programs	53			X	X				X		
AA 98-200	Special Access Programs	53	X	X	X	X						
AA 98-353	Reynolds Army Community Hospital	54		X		X			X	X		X
AA 98-367	SIDPERS-3	55	X		X		X		X	X		
AA 98-366	Arlington National Cemetery	55	X	X	X	X				X		X
AA 98-351	Patterson Army Health Clinic	56	X		X							X
AA 98-347	Winn Army Community Hospital	56		X						X		X
AA 98-332	Army Reserve	56	X	X	X	X	X		X	X		X
AA 98-363	U.S. Army Europe and Seventh Army	57	X			X	X	X	X	X		
AA 98-335	Army Recreation Machine Program	58					X		X	X		
AA 98-342	Darnall Army Community Hospital	58							X	X		X

Report No.	Organization/ Function	Ap.B Page	Over.& Awar.	Report.	Assess.	Resour. Est.	Interf.	Priorit.	Testing	Cont.& Coop.	Ctracts.	Infrast.
AA 98-348	William Beaumont Army Medical Center	58	X	X					X	X		X
AA 98-344	Tripler Army Medical Center	59	X			X			X	X		X
AA 98-355	Morale, welfare, and recreation	60			X				X	X	X	X
AA 98-354	Morale, welfare, and recreation	60							X	X		
AA 98-349	Eisenhower Army Medical Center	61	X						X	X		X
AA 98-352	Fox Army Health Center	61		X	X					X	X	X
AA 98-345	Madigan Army Medical Center	61								X		X
AA 98-346	Evans Army Community Hospital	62	X		X				X	X		X
AA 98-343	Brooke Army Medical Center	62	X	X						X		X
AA 98-331	Combat Service Support	62					X		X			
AA 98-327	Morale, welfare, and recreation Division	63	X	X	X	X						X
AA 98-328	Morale, welfare, and recreation	63	X		X	X			X	X		X
AA 98-326	Morale, welfare, and recreation	64							X	X		
AA 98-322	Army Reserve Personnel Command	65	X	X	X	X	X			X		
AA 98-321	All Source Analysis System	66		X			X					
AA 98-311	Army	66	X	X	X		X		X	X		
AA 98-310	TC-AIMS II	67		X			X		X			
AA 98-309	Army Reserve Command	67	X	X	X	X	X			X		
AA 98-291	U.S. Southern Command	67	X	X	X		X		X	X		
AA 98-292	U.S. European Command	68	X	X	X		X			X		
AA 98-213	U.S. Naval Forces Europe	69	X	X	X		X	X		X		
AA 98-221	Deputy Chief of Staff for Operations and Plans	70	X		X	X	X			X		
AA 98-220	Program Analysis & Evaluation Directorate	70	X		X		X		X	X		

Report No.	Organization/ Function	Ap.B Page	Over.& Awar.	Report.	Assess.	Resour. Est.	Interf.	Priorit.	Testing	Cont.& Coop.	Ctracts.	Infrast.
AA 98-219	Army Deputy Chief of Staff for Intelligence	70	X		X				X	X		
AA 98-218	Army Deputy Chief of Staff for Personnel	70			X				X	X		
AA 98-217	Army Deputy Chief of Staff for Logistics	70	X		X		X		X	X		
AA 98-216	Army Chief of Staff for Installation Management	70	X		X	X	X		X	X		
AA 98-215	Assistant Secretary of the Army (FM&C)	70	X		X	X	X		X	X		
AA 98-214	Assistant Secretary of the Army (M&RA)	70	X		X		X		X	X		
AA 98-212	Assistant Secretary of the Army (RD&A)	70	X		X	X	X		X	X		
AA 98-197	Army C^3 Systems	71	X	X	X					X		
AA 98-194	Army Corps of Engineers	72	X	X	X		X	X	X	X		
AA 98-227	Army National Guard	72	X	X	X	X	X		X	X		
AA 98-167	SIDPERS-3	73	X	X	X		X		X	X		
AA 98-176	ATRRS	75	X	X		X	X		X	X		
AA 98-175	AIMS-R	76										
AA 98-107	U.S. Army Europe and Seventh Army	76	X	X	X	X	X		X	X		
AA 98-122	Standard Army Retail Supply System	77					X			X		
AA 98-128	Global Command and Control System-Army	77		X	X	X	X			X		
AA 98-127	Adv. Field Artillery Tactical Data System	78		X	X		X			X		
AA 98-118	Army Training and Doctrine Command	79	X	X	X		X		X	X		X
AA 98-115	Forces Command	79	X	X	X		X			X		
AA 98-120	Army	80	X	X	X				X	X		
AA 98-116	Eighth Army	80	X	X	X	X			X	X		
AA 98-100	Army	81	X		X	X	X		X	X		
AA 98-36	Army	81	X		X							

Report No.	Organization/ Function	Ap.B Page	Over.& Awar.	Report.	Assess.	Resour. Est.	Interf.	Priorit.	Testing	Cont.& Coop.	Ctracts.	Infrast.
Inspector General, Navy												
Not Numbered	Naval Reserve Force	82	X	X	X		X		X	X		X
Not numbered	Navy	83	X	X	X	X	X		X			
Naval Audit Service												
Memorandum	Naval Air Systems Command	84	X	X	X	X	X		X	X		X
Memorandum	Naval Sea Systems Command (Team CX)	84	X	X	X	X	X		X	X	X	X
Memorandum	Naval Sea Systems Command	85	X	X	X	X	X			X	X	X
Memorandum	Naval Air Systems Command	86	X	X	X	X	X			X	X	X
Memorandum	Navy Undersea Warfare	86	X	X	X	X	X		X	X	X	X
Memorandum	Naval War College	87		X	X		X					X
Memorandum	Operations Naval Support Activity	87	X	X	X		X		X	X		X
Memorandum	Naval Academy	88	X		X				X	X		X
Memorandum	Naval Strike and Air Warfare Center	89	X	X	X				X	X		X
Memorandum	SPAWAR	89	X	X	X	X	X	X	X	X		X
Memorandum	Naval Sea Systems Command	90	X	X	X		X		X	X		X
Memorandum	Naval Sea Systems Command for MW	91	X	X	X		X		X	X		X
Memorandum	Naval Safety Center	92	X	X	X		X		X	X		X
Memorandum	Naval Legal Services Command	92	X	X	X				X			
Memorandum	President Board of Inspection and Survey	93	X	X	X	X	X		X	X	X	X
Memorandum	Naval Meteorology and Oceanography Command	93	X	X	X		X			X		X
Memorandum	Naval Reserve Forces	94	X	X	X	X	X		X	X	X	
Memorandum	Chief of Naval Education and Training	94	X		X		X			X	X	X
Memorandum	Naval Air Systems Command	94	X	X	X	X	X		X	X		

Report No.	Organization/ Function	Ap.B Page	Over.& Awar.	Report.	Assess.	Resour. Est.	Interf.	Priorit.	Testing	Cont.& Coop.	Ctracts.	Infrast.
Memorandum	Naval Historical Center	95			X		X			X		
Memorandum	Naval Observatory	95								X		
Memorandum	Navy Field Support Activity	96	X		X				X	X		X
Memorandum	Navy Tactical Support Activity	96	X									
Memorandum	Naval Supply Systems Command	96		X	X		X					
Air Force Audit Agency												
98066033	U.S. Strategic Command	97				X						
98066032	U.S. Transportation Command	97			X					X		
98066019	Air Force Phase Status Validation	98	X	X	X	X	X		X	X	X	
97066036	Air Force Systems Assessment	100			X		X	X		X		
97066018	Air Force Inventory Status	100	X	X	X							
Inspector General, Marine Corps												
Summary	Marine Corps	101	X	X	X	X	X	X	X	X		X

Ap. B Page	Appendix B Page Reference
Over. & Awar.	Oversight and Awareness
Report.	Reporting
Assess.	Assessment
Resour. Est.	Resource Requirements Estimation
Interf.	Interface Identification and Agreements
Priorit.	Prioritization
Cont. & Coop.	Contingency and Continuity-of-Operations Planning
Ctracts.	Contracts
Infrast.	Infrastructure

Adv.	Advanced
AF	Air Force
AIMS-R	Automated Instructional Management System-Redesign
AMR	Army Medical Research
ATRRS	Army Training Requirements and Resources System
AWACS	Airborne Warning and Control System
BMDO	Ballistic Missile Defense Organization
C^3	Command, Control, and Communications
Comm.	Communications
DARPA	Defense Advanced Research Projects Agency
Dep	Deputy
DIST	Defense Integration Support Tools
DISA	Defense Information Systems Agency
Eval.	Evaluation
FM&C	Financial Management and Comptroller
IT	Information Technology
JBC	Joint Battle Center
JC2WC	Joint Command and Control Warfare Center
JCSE	Joint Communications Support Element
JWAC	Joint Warfare Analysis Center
JWFC	Joint Warfighting Center
M&RA	Manpower and Reserve Affairs
MW	Mine Warfare
RD&A	Research, Development, and Acquisition
SAP	Special Access Program
SIDPERS	Standard Installation and Division Personnel System
SPAWAR	Space and Naval Warfare Systems Command
TC-AIMS	Transportation Coordinators-Automated Information for Movement System

Appendix B. Synopsis of Year 2000 Issues

Following are summaries of the Y2K issues detailed in audit and inspection reports. At the end of each summary, we describe the status of any agreed-upon management actions, documented as of December 1998.

General Accounting Office

Report No. AIMD-98-124 (OSD Case No. 1672), "Year 2000 Computing Crisis: Actions Needed on Electronic Data Exchanges," July 1, 1998. The report states that Federal agencies did not complete key actions to address Y2K data exchange issues. In January 1998, the Office of Management and Budget issued instructions requiring Federal agencies to inventory all data exchanges with outside parties by February 1, 1998, and coordinate the resolutions with the exchange partners by March 1998. However, no actions had been taken to establish target dates for testing the new data exchange format or developing and implementing contingency plans. Most Federal agency actions to address Y2K issues with the international data exchanges were to be directed to the financial services areas. As part of the correction efforts, organizations were to identify the date format used in their data exchanges, develop a strategy for dealing with the exchanges that do not use four-digit year formats, and implement the strategy. Also, testing and implementation of the new data exchange was to be closely coordinated with exchange partners to be completed effectively. The report identifies DoD as one of three Federal agencies that had a large number of foreign entities. DoD had identified 103 foreign data exchanges, yet agreements of understanding had only been completed for 18 of the data exchanges. Because the report is Government-wide and the Office of Management and Budget is the responsible agency for Y2K data exchanges, the report made no recommendations to DoD management.

Report No. AIMD-98-150 (OSD Case No. 1622), "Defense Computers Year 2000 Computer Problems Put Navy Operations at Risk," June 30, 1998. The review was conducted from August 1997 through April 1998. The report states that the Y2K program of the Navy lacked key management and oversight controls needed to enforce good management practices, direct resources, and establish accountability. As a result, the Navy had not developed a comprehensive department-wide inventory of systems, prepared interface agreements, developed a test strategy, or prepared contingency plans.

Management concurred and prepared a corrective action plan addressing the issues cited in the report. The corrective action plan included the following:

- establishing a complete and accurate inventory,

- ensuring that DoD Components identify and correct interfaces and develop written memorandums of agreement with the interface partners,

- developing a Navy-wide test strategy that would describe the roles and responsibilities of all organizations and personnel involved, and

- focusing Y2K contingency planning on the continuity of all Navy critical military operations and business processes.

Report No. AIMD-98-53 (OSD Case No. 1572), "Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program," May 29, 1998. The review was conducted from November 1996 through February 1998. The report states that the Y2K program of the Army lacked management and oversight control. As a result, the Army did not have complete and accurate information regarding systems, interfaces, and cost estimations. Also, interface agreements and contingency plans had not been developed nor had test resources been identified. Therefore, the Y2K program of the Army risked failure because the data required to effectively manage corrective actions were incomplete, inaccurate, or undetermined.

Recommendations to the Secretary of the Army required Army components to:

- correct their inventory databases,

- certify all claims of Y2K compliance and submit the completed certification checklist to the Army Y2K Project Office,

- provide reliable Y2K cost estimations based on a comprehensive inventory and completed assessments of all mission-critical systems so that priorities can be established and important trade-off decisions can be made,

- prepare contingency plans that include specific actions for Y2K operations,

- prepare interface memorandums for all interfaces identified, and

- develop test plans and identify any additional resources needed.

In addition, the report required that the Army Y2K Project Office ensure that the Army Y2K database contained complete, accurate, and current information. The report required the project office to monitor components' progress in identifying system interfaces and defining details of data exchanges between system interfaces and the progress of the preparation and implementation of the required memorandums of agreement. Also, the project office was required to negotiate the schedule of test facilities if needed.

The Army commented that actions were already in progress to improve the Army Y2K program, citing a February 1998 policy memorandum as an example of the improvement actions. The memorandum directed components to provide more complete and accurate data on their systems, ensure that all mission-critical systems and major systems reported as compliant are certified and copies of the certification are provided to the Army Y2K Project Office, ensure that all noncompliant mission-critical systems and major systems are certified following renovation and testing, complete contingency plans for mission-critical systems and major systems and core business areas, and inventory all system interfaces and coordinate interface agreements with interface partners. Also, the

memorandum directed senior-level component managers to meet with the Chief Information Officer during April and May 1998 to review progress in fixing Y2K issues. Until actions to implement all the recommendations were completed, the Army could not ensure that the transition into the next millennium would not be disrupted.

Report No. AIMD-98-85, "Year 2000 Computer Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships," April 30, 1998. The report recaps findings from more than a dozen General Accounting Office reports regarding the status of the Federal Government Y2K readiness. The report states that many agencies were still vulnerable to Y2K disruptions because they were behind schedule, and more action is needed to ensure that Y2K risks would be mitigated and debilitating consequences avoided. Because a high degree of information and systems interdependence existed among various levels of Government and the private sector, the interdependencies increased the risks that failures or interruptions of essential services could occur. Additionally, time was rapidly winding down for the Federal Government to set priorities to focus Y2K efforts on the most important systems and to ensure that the systems receive appropriate testing. As a result, any uncertainties regarding Y2K compliance for agencies' internal systems, systems of the data partners, and systems that support the public infrastructure made developing and testing contingency plans an essential task. Further, to make informed decisions, complete and timely information of the Federal Government Y2K readiness must be reliable. Therefore, agencies were to report progress regularly, expand reporting elements, and set independent verification standards for agency efforts. The report states that the DoD Y2K Program lacked key management and oversight controls to enforce good management practices, to direct resources, and to establish a complete picture of its progress in fixing systems. Recommendations made to the Secretary of Defense were as follows:

- establish a strong DoD-level program office;
- expedite efforts to establish a comprehensive, accurate DoD-wide inventory of systems, interfaces, and other repairs needed;
- clearly define criteria and an objective process for prioritizing systems for repair based on their mission-criticality;
- ensure that system interfaces are adequately addressed;
- develop an overall, DoD-wide testing strategy and a plan for ensuring that adequate resources are available to perform necessary testing;
- require DoD Components to develop contingency plans; and
- prepare complete and accurate Y2K cost estimates.

The DoD management concurred with the recommendations. Specific recommendations were made to Logistics Systems Support Center, the Air Force, the Defense Finance and Accounting Service, and the Defense Logistics Agency for improvements to the Y2K programs, including the need to develop contingency plans.

Report No. AIMD-98-72 (OSD Case No. 1562), "Defense Computers: Year 2000 Computer Problems Threaten DoD Operations and National Security," April 30, 1998. The review was conducted from August 1997 through February 1998. The report discusses the General Accounting Office assessment of the DoD effort to identify and correct its Y2K problem and the strategy and actions needed to resolve the problem. Specifically, the report states the systemic weaknesses in the DoD Components' Y2K programs. The systemic weaknesses identified were in the following areas:

- effective oversight and management of Y2K remediation efforts,
- accurate and complete system inventory,
- system prioritization for correction,
- proper addressing of interfaces,
- preparation for testing,
- contingency planning, and
- reliable cost information.

The report recommended the following to the Secretary of Defense:

- establish a program office led by an executive manager assigned with the full-time responsibility to manage and oversee Y2K efforts;
- expedite efforts to establish an accurate and comprehensive system inventory, record of all interfaces, and inventory of equipment needing repair. Also, require DoD Components to validate the accuracy of the Y2K data reported;
- clearly define the prioritization process for systems needing repairs based on their mission criticality;
- implement system interface guidelines to include completing the inventory and assigning responsibility for each system, tracking Y2K resolutions, requiring interface documentation, and providing guidance on the content of interface agreements;
- develop a testing strategy outlining the test criteria and processes to be used and ensure that adequate resources exist to perform testing;
- require DoD Components to develop contingency plans and track DoD Components' progress in completing the plans; and
- develop complete and accurate Y2K cost estimates.

DoD management concurred with all findings and recommendations and took corrective actions as directed by the recommendations. A full-time executive was appointed to lead the efforts to solve the Y2K challenge. DoD initiated action to immediately establish an unclassified Y2K interactive database to collect

validated information to evaluate progress and provide quarterly reports to the Office of Management and Budget. In addition to defining the term "Y2K system" in a March 12, 1997, memorandum, the term is officially defined in the Joint Publication 1-02, and both documents provide specific guidance. Although the guidance for prioritizing systems contained in the initial DoD Management Plan is rather broad, the Draft DoD Management Plan provided expanded direction on the process of prioritizing systems for repair based on DoD needs and mission. Since the issuance of the audit report, progress had been made in identifying interfaces, both external and internal. Also, the report process that DoD developed in response to the Office of Management and Budget was put in place. Additionally, the format for memorandums of agreement with interface partners had been defined and was to be formalized in the Draft DoD Management Plan. Further, the Defense Information Systems Agency and the Joint Interoperability Test Command had developed a series of testing conditions for use in determining Y2K compliance. Also, DoD Components were required to prepare a DoD Component-wide master contingency plan that would allow continued operation should failure result because of the Y2K problem. As a result, DoD developed its contingency plan in accordance with the new General Accounting Office "Y2K Computing Crisis: Business Continuity and Contingency Planning" document. The plan was based on several disaster scenarios, including the failure of the national infrastructure that provides power to the facilities. Also, the contingency plans were to be reviewed quarterly. Further, DoD adopted the algorithms that private industry developed to estimate Y2K costs, but the DoD Components had to provide actual costs as they became available. The estimates were used to assess the impact of the Y2K problem and, through the DoD Y2K Steering Committee, make trade-off decisions as needed to fund repairs of mission-critical systems. Consequently, DoD would be sure that adequate resources were available for Y2K.

Report No. AIMD-98-35 (OSD Case No. 1484), "Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight," January 16, 1998. The review was conducted from July 1996 through August 1997. The report discusses the Air Force Y2K program. Issues identified in the General Accounting Office review include inadequate cost estimates, limited accountability of interfaces, timely development of contingency plans, and planning the test phase.

The report recommended that the Secretary of the Air Force ensure that cost estimates factor in the actual resources believed to be needed for renovating or implementing Y2K repairs. The Air Force also was to develop an approach to track the process that would be used to identify interfaces, correct interfaces, institute memorandums of agreement, develop test plans, identify the need for additional testing, and obtain any needed testing resources. Finally, the Air Force was to ensure that its components prepared contingency plans for all mission-critical systems. The Air Force agreed with the report's findings and recommendations.

Air Force officials agreed to update cost estimates, including the costs related to the actual resources used as they progress through the remaining Y2K phases. Also, Air Force personnel stated that greater management interest would be placed in identifying system interfaces and improving reporting practices. Further, the Air Force agreed to prioritize test requirements to ensure that testing resources would be available when needed.

The Air Force already began implementing actions to improve its Y2K program. For example, components were working to develop contingency plans as part of the renovation and validation phases. The Air Force planned to open Service-wide crisis response centers to deal with critical systems that would not be Y2K compliant by August or September 1999. As result, the Air Force expected contingency plans to be prepared for each noncompliant system and the information to be made available to the crisis response centers.

Based on direction from the Secretary of the Air Force and the Air Force Chief of Staff, Y2K is the number one software sustainment issue of the Air Force. Consequently, program managers were directed to defer all nonessential sustainment and modernization activities until Y2K issues were resolved. Also, the managers were tasked to develop and refine realistic cost estimates during the assessment and renovation phases.

Report No. AIMD-98-7R (OSD Case No. 1471), "Defense Computers: Technical Support Is Key to Naval Supply Year 2000 Success," October 21, 1997. The report states that the Naval Supply Systems Command made sufficient progress with its Y2K program but did not allocate sufficient resources to ensure that all system interfaces were identified and adequately monitored. Also, the Naval Supply Systems Command did not prepare risk assessments or contingency plans to minimize the loss of operational capability in Y2K. Therefore, the report concludes that the Naval Supply Systems Command needed to maintain its current level of effort and discipline in managing its Y2K program to improve the management approach as new and unanticipated issues arise. The DoD management concurred.

Management assigned full-time staff to identify the related interface files and the date-related elements and planned to issue letters to the interfacing organizations proposing a format that is compatible with the systems' internal processes. As a result, management agreed to require system mangers to perform risk assessments and to prepare contingency plans for critical systems. The risk-management plan recognizes the risks associated with interfacing with third parties and the need to analyze areas such as the corporate strategy, human resources, project management, and systems implementation to ensure the continuity of operations. Further, the functional and the system levels would prepare the contingency plan to minimize the loss of operational capability.

Report No. AIMD-97-149 (OSD Case No. 1446), "Defense Computers: Logistics Systems Support Center (LSSC) Needs to Confront Significant Year 2000 Issues," September 26, 1997. The report states that the Logistics Systems Support Center (the Center) did not completely address the critical issues of prioritizing workload and staffing needs, developing a test strategy, identifying the scope and substance of interface agreements, and preparing operational contingency plans for Y2K. As a result, the procurement of weapon systems and spare parts, the accountability of sales to allies, and the financial management of $9 billion of inventory could be disrupted. Recommendations to the Office of the Under Secretary of Defense for Acquisition and Technology included improving the Center's software development process to lead to achieving a capability maturity model level 2 rating. Also, the report recommended that the workload and staffing demands be assessed and, based on the assessment, that management make the appropriate decisions to ensure timely completion of the Y2K project. The Center should have the capability to complete testing, prepare detailed

interface agreements, and develop a contingency plan that includes specific actions for continuing operations without disruption. DoD concurred with all recommendations.

DoD initiated actions to reduce and prioritize the Center's current workload and to increase staff with skills to help ensure timely completion of the Y2K project. Further, DoD took actions to improve its capability to complete Y2K testing. The actions included the completion of a draft test plan, placement of a contractor on site to assist in the development of the final test plan, establishment of a new Y2K test team to formulate a test approach, and creation of a separate domain for Y2K work and testing. DoD stated that the Center would meet the mandates for the Defense base realignments and closures and Y2K projects before resuming efforts to achieve a capability model maturity level 2 status because having a higher level of maturity is key to reducing the risk of schedule slippage, cost overruns, and poor software quality. Also, DoD stated that the Center formalized memorandums of agreement with interface partners and included specific detailed information as needed to ensure that interface partners are sufficiently prepared to handle unforeseen problems and plans for contingencies. Consequently, the Center completed its initial contingency plan and forwarded it to the system functional proponents for action. The contingency plan was expected to be a living management tool that would be maintained and updated for the life of the project.

Report No. AIMD-97-120R (OSD Case No. 1399), "Defense Computers: Standard Systems Group (SSG) Needs to Sustain Year 2000 Progress," August 19, 1997. The report states that the Air Force Standard Systems Group (the Group) must further emphasize management oversight of systems interfaces to ensure that the implementation of Y2K compliant systems would be successful. The Group's systems were to develop interface agreements to address the use of standard interface message formats to exchange data. As a result, the report states that the Group management would need to maintain the same level of effort and discipline and continue to improve its management approach as new or unanticipated issues arise. Although the report made no recommendations, the Air Force agreed with the findings and stated they verify similar findings that the Air Force Audit Agency identified. The Air Force responded that fixing Y2K was its top software sustainment issue, and it would be fixed before anything else. The Air Force stated that it hoped to complete the Y2K solutions by January 1, 1999, and have a year to resolve the interface issue and other unforeseen problems.

Report No. AIMD-97-112 (OSD Case No. 1395), "Defense Computers: Improvements to DoD Systems Inventory Needed for Year 2000 Effort," August 13, 1997. The report discusses the inaccuracy of the inventory information contained within the Defense Integration Support Tools database. Without a complete inventory, DoD as a whole could not adequately assess department-wide progress for correcting the Y2K problems nor manage the Y2K effort. If DoD did not give immediate attention to obtaining an inventory of each system for each business area, DoD Y2K efforts would be at risk of failing. The report recommended that DoD direct the staff to oversee implementation of the DoD Management Plan. Also, the report recommended that the Defense Information Systems Agency identify and investigate duplicate, inactive, and incomplete entries and that the DoD staff and the Defense Information Systems Agency expedite development and implementation of the purging methodology

and expand Y2K information to include key program activity. DoD concurred and responded that it would validate the accuracy of the inventory data contained within the Defense Integration Support Tools database using statistical sampling and would confirm the accuracy during the Y2K audits conducted by the Office of the Inspector General, DoD. Also, the Defense Information Systems Agency instituted a data quality program purging duplicative and obsolete data. However, DoD stated that the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) needed to supplement the actions by requiring that inventories of the Services and the DoD Components be reconciled with the Defense Integration Support Tools database. Further, the management involved was to play an active role in ensuring that data fields needed to track Y2K progress were included in the upgraded Defense Integration Support Tools database.

Report No. AIMD-97-106 (OSD Case No. 1389), "Defense Computers: Issues Confronting Defense Logistics Agency (DLA) in Addressing Year 2000 Problems," August 12, 1997. The report states that the Defense Logistics Agency did not complete the assessment phase of Y2K. It did not develop the interface memorandums needed to provide information about date format. Also, the Defense Logistics Agency did not include system-unique programs in the system inventory, prioritize mission-critical systems for repair, or develop contingency plans detailing the course of action to be followed in the event of Y2K disruptions. The report recommended that the Defense Logistics Agency require written interface agreements detailing its expectations with interface partners, ensure that unique applications or systems are included in the Y2K inventory, determine whether all systems have a Y2K issue, and ensure that all inventoried systems are compliant. Also, the report recommended that the Defense Logistics Agency develop a Y2K system prioritization process and develop and issue contingency plans for all critical systems. DoD concurred with the recommendation on interface agreements and contingency plans and partially concurred with the recommendation on the unique applications or systems. However, the Defense Logistics Agency did not concur with the recommendation on the systems prioritization process and stated that the mission-critical systems were undergoing remediation efforts concurrently using in-house and contractor resources, and progress was being made toward the completion of the efforts that were expected to be completed on time. Further prioritization beyond what was established was not needed at that time.

Report No. AIMD-97-117 (OSD Case No. 1392), "Defense Computers: Defense Finance and Accounting Service (DFAS) Faces Challenges in Solving the Year 2000 Problem," August 11, 1997. The report states that the Defense Finance and Accounting Service did not address critical issues related to identifying the critical tasks necessary to complete Y2K tasks; performing a formal risk assessment of all systems and ensuring that contingency plans were developed; identifying all system interfaces, including the external interfaces; and ensuring that testing resources were available when needed. If the Defense Finance and Accounting Service did not address the critical issues, the systems could fail to operate in Y2K. Recommendations were that the Defense Finance and Accounting Service build on the existing plan to ensure that actions were established and schedules of completion were identified; prepare contingency plans to address the Y2K crisis and additional guidance to require management to perform risk assessments; require that timely identification of internal and external system Y2K compliance be based on the testing of all systems; and

devise a test schedule that identifies all test resources and facilities. DoD concurred with all recommendations and developed a Y2K management plan to identify its actions and schedules for completing each phase of the Y2K program. In addition, the Defense Finance and Accounting Service was updating the contingency plan to require a risk assessment and business impact analysis of all mission-critical systems. Testing was mandated for all Defense Finance and Accounting Service systems for Y2K compliance, and the Defense Finance and Accounting Service directed its managers to establish written interface agreements with all interface partners. Further, the Defense Finance and Accounting Service intended to implement its mandatory Y2K certification process as outlined in the updated Defense Finance and Accounting Service Y2K Management Plan. The Defense Finance and Accounting Service stated that it would develop a testing schedule to identify the test facilities and resources needed to test Defense Finance and Accounting Service systems.

Office of the Inspector General, DoD

Inspector General, DoD, Report No. 99-058, "Year 2000 Conversion of Defense Critical Suppliers," December 18, 1998. The report states that until late FY 1998, outreach efforts to suppliers of national Defense goods and services were left to individual DoD Components to organize, execute, and monitor. As a result, the emphasis put on outreach to suppliers varied greatly among DoD acquisition and logistics organizations. The report states that DoD faces an increased risk of production and delivery disruptions because of the belated outreach focus to ensure suppliers' Y2K conversion. Further, the report states that if commercial suppliers of critical supplies experience disruptions as a result of computer failures, the logistics pipeline may be compromised.

The report states that the Deputy Under Secretary of Defense (Logistics) had taken a positive approach to developing a more systematic assessment of the critical suppliers' Y2K compliance by establishing a Joint Supplier Capability Working Group as a forum on this issue. As of October 1998, the Joint Supplier Capability Working Group had established the methodology for identifying critical items as well as their supplier, and a reasonable action plan for assessing critical suppliers' Y2K compliance. The report concludes that a sustained effort by the Joint Supplier Capability Working Group was needed to compensate for the belated focus on this aspect of the Y2K conversion challenge and to ensure a proper evaluation of the critical suppliers' ability to provide critical items into the Y2K and beyond. The report made no recommendations.

Inspector General, DoD, Report No. 99-055, "Year 2000 Computing Issues Related to Health Care in DoD," December 15, 1998. The report states that the Assistant Secretary of Defense (Health Affairs) and the Military Departments have taken many positive actions to identify and correct Y2K problems in the Military Health Systems automated information systems, biomedical devices, and facility devices. However, the report states that the Assistant Secretary of Defense (Health Affairs) action needed to take additional action for the area of automated information systems.

The report recommended that the Assistant Secretary of Defense (Health Affairs) establish procedures to promptly report slippage in completion dates; prepare interface agreements and contingency plans in accordance with the DoD Management Plan; and make sure slippage does not occur when Y2K fixes are combined with system upgrades. Additionally, the Assistant Secretary should appropriately test to mitigate the risks for products obtained recently on contracts and delivery orders that did not include required Y2K clauses. The report also recommend that the Assistant Secretary perform tests, where possible, of biomedical devices for Y2K compliance, and issue direction to the Military Department Surgeons General that require military treatment facility commanders to coordinate with installation commanders to ensure the appropriate priority is given to medical facility devices in the Y2K compliance process. The Principal Deputy Assistant Secretary of Defense (Health Affairs) concurred with the finding and recommendations and took corrective action.

Inspector General, DoD, Report No. 99-052, "Year 2000 Conversion of Logistics and Maintenance Systems in Support of the Airborne Warning and Control System," December 11, 1998. The report states that the Air Force Materiel Command established a Y2K corrective program and took positive actions to address and resolve its Y2K problem. However, the Oklahoma City and San Antonio Air Logistics Centers had not always prepared documented contingency plans, test plans and results, and certifications to support the Y2K progress reported. The situation occurred because the Air Logistics Centers did not effectively monitor the accuracy of the status of progress reported by the system managers. The report states that unless the Air Logistics Centers make further progress ensuring the accuracy of Y2K status reported, the Airborne Warning and Control System and possibly other weapon systems face increased risk that Y2K-related disruptions in computer operations will impair their mission capabilities.

The report recommended that the Oklahoma City and San Antonio Air Logistics Centers direct system managers to prepare and make available documentation to certify Y2K compliance of logistics and maintenance systems. Specifically, the report recommended that the system managers prepare contingency plans, test plans, test results, and interface agreements before certifying that a system is Y2K compliant. The systems managers also were to prepare a certification tracking document and a certification checklist to ensure that the necessary documents were prepared. The Air Force did not provide comments to the report.

Inspector General, DoD, Report No. 99-049, "Year 2000 Contingency Planning and Cost Reporting at the Defense Finance and Accounting Service," September 25, 1998. The report states that the Defense Finance and Accounting Service had good corporate level focus and guidance for contingency planning. However, most system managers had not yet established adequate Y2K contingency plans and reliable cost estimates.

Contingency Plans. System-level contingency plans did not adequately address methods for conducting business operations in the event of a Y2K system failure. Systems for which the Defense Finance and Accounting Service is a minority owner did not have contingency plans that adequately addressed alternative work processes for maintaining continuity of Defense Finance and Accounting Service business functions. Contingency plans were inadequate because system managers did not have sufficient guidance to establish a

contingency plan. Additionally, the Defense Finance and Accounting Service decided to focus efforts on identifying, assessing, and changing systems affected by the Y2K problem, rather than on establishing contingency plans.

The report states that of the 29 mission-critical, migratory, and payment systems selected for review, 21 systems had contingency plans. The report states that although many Defense Finance and Accounting Service system managers were able to provide written documentation for a contingency plan, nearly all plans lacked the basic information needed to implement and manage a Y2K-related contingency. The plans did not include elements such as risk assessment, processing alternatives, trigger procedures, staff roles, and contingency-plan testing. Further, the contingency plans did not have an adequate evaluation of the magnitude and complexity of the systems, or a detailed description of manual procedures. During the review, the Defense Finance and Accounting Service Director, Information and Technology, responded to the issues concerning contingency plans. The Director agreed with the issues identified, and in a memorandum, discussed actions underway to correct deficiencies in the contingency plans for all critical systems and systems that feed critical systems. Additionally, the Defense Finance and Accounting Service issued Y2K Contingency Planning guidance that addressed the necessary elements for contingency plans as outlined in the General Accounting Office's "Y2K Computing Crisis: Business Continuity and Contingency Planning," August 1998.

The report recommended that the Defense Finance and Accounting Service:

- establish a verification mechanism to ensure that system managers had developed contingency plans that meet the requirements of the Defense Finance and Accounting Service Y2K Contingency Planning Guidance, and

- ensure that the Defense Finance and Accounting Service minority-owned systems had adequate contingency plans addressing the Defense Finance and Accounting Service business processes.

The Defense Finance and Accounting Service concurred and stated that the Defense Finance and Accounting Service Contingency Planning guidance requires that Y2K contingency plans be reviewed and signed by the systems manager, Center Director, and headquarters functional representative. Also, the Defense Finance and Accounting Service Y2K Project Officer was to track the completion of the required contingency plans. In addition, to ensure that the Defense Finance and Accounting Service jointly owned systems had adequate contingency plans addressing the Defense Finance and Accounting Service business processes, the Defense Finance and Accounting Service was to develop Core/Core Support Business Process contingency plans.

Cost Reporting. The report states that the Defense Finance and Accounting Service reported incomplete Y2K costs and underreported Y2K cost estimates in the Office of Management and Budget Quarterly Report. The inaccuracies occurred because the Defense Finance and Accounting Service did not include all of the necessary cost elements identified in the DoD Management Plan.

During the review, the Defense Finance and Accounting Service agreed that the initial cost estimates were incomplete and did not include all necessary elements identified in the DoD Management Plan. The Defense Finance and Accounting Service implemented the corrective actions to address the incomplete cost estimates.

Inspector General, DoD, Report No. 99-046, "Year 2000 Initiatives at the Army Kwajalein Missile Range," December 4, 1998. The report states that Kwajalein Missile Range actions to resolve and report on systems having potential date-processing issues were improving. The report states that the audit identified that three systems, the Target Resolution and Discrimination Experimental Radar System, the Mobile Radar Search 36 System, and the Kwajalein Mobile Range Safety System, lacked a Y2K assessment of mission-critical subsystems, that cost estimates and the budget impact were outdated, and that the Kwajalein Missile Range did not have a risk-management plan with a prioritized list of affected systems. As a result, the Kwajalein Missile Range officials moved the three systems back to the assessment phase; initiated actions to update cost estimates and their impact on the budget; and agreed to develop a risk-management plan that included a list of prioritized systems.

Additionally, the report states that the Kwajalein Missile Range took positive steps to assign an independent agent to review test plans and analyze the results to ensure that test and evaluation systems would be Y2K compliant. Officials also agreed to prepare a contingency plan by March 1999 for mission-critical systems that would not be Y2K compliant by December 1998. As a result, there was an increased confidence in the range test plans, test results, and the continued functions of the systems after 1999. The report concludes that because management took corrective action during the audit, no recommendations were necessary.

Inspector General, DoD, Report No. 99-039, "552nd Air Control Wing Year 2000 Infrastructure Program for the Airborne Warning and Control System," November 23, 1998. The report states that the 552nd Air Control Wing (the Wing) did not prepare a program management plan that encompassed guidance from DoD, the Air Force, and the Air Combat Command. The Wing also had not identified all mission-critical and mission-essential infrastructure systems. The conditions occurred because the Wing did not take a proactive role in the oversight of Y2K conversion and the implementation of Air Force Y2K guidance. As a result, the Wing was unable to prioritize its resources for fixing Y2K problems and could not provide assurance that Airborne Warning and Control System mission-critical and mission-essential infrastructure systems would be operational in the Y2K and beyond. The report concludes that, without that assurance, the operational availability of the Airborne Warning and Control System could be affected.

The report recommended that the Wing appoint a Y2K management team that includes senior management officials from the operations, logistics, and computer systems functional groups to provide oversight and direction for the Y2K program. The management team would require the Y2K working group to revise the program management plan so that it effectively addressed contingency and test plans, certification procedures, and reporting requirements. Additionally, the report recommended that the Y2K management team identify mission-critical and

mission-essential infrastructure systems and prioritize those systems for repairs, renovation, or replacement. The Commander, 552nd Air Control Wing, concurred and took corrective action.

Inspector General, DoD, Report No. 99-038, "Year 2000 Initiatives at the Pacific Missile Range Facility," November 23, 1998. The report states that the Navy officials at the Pacific Missile Range Facility initiated positive actions to accurately report all systems' monthly status to DoD to estimate the cost to fix or replace systems that were not Y2K compliant and report any adverse budget impacts. The actions occurred after the audit team identified that systems on the Pacific Missile Range Facility boats were not included in the monthly DoD status report and that costs estimates and the budget for fixing noncompliant test and evaluation systems and their budget impact were not prepared. Navy officials agreed to inventory systems on their boats, prepare cost estimates and potential budget impacts for fixing the Y2K problem on affected systems, and report results on the next monthly report to DoD. The report made no recommendations.

Inspector General, DoD, Report No. 99-036, "Army Research Laboratory Preparation for the Year 2000," November 13, 1998. The report states that the Army Research Laboratory had not met the required time frames of the Army Y2K Action Plan for identifying and assessing Y2K problems. Additionally, the Army Research Laboratory had not done the following.

- The Army Research Laboratory did not develop the comprehensive inventory of hardware; software, and firmware systems required by the Army Y2K Action Plan. Although officials distributed Y2K questionnaires for an initial inventory of systems and an assessment of the Y2K impact on its systems, personnel did not respond to the questionnaire.

- The Army Research Laboratory did not assess all ongoing research programs and their potential system interfaces or the systems to which the research programs applied. The Army Research Laboratory identified and assessed only 10 of 460 ongoing research efforts. Management officials stated that program managers or engineers did not examine the remaining programs because the managers believed that the programs were too early in the development process to be assessed for Y2K compliance.

- The Army Research Laboratory did not include the Y2K clause for 17 of 29 randomly selected contracts. The randomly selected contracts were pulled from 175 contracts issued for a 22-month period ending July 1998. Contracting officials stated that they did not formally review all information technology contracts as directed in the December 18, 1997, memorandum from the Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

The report recommended that the Army Research Laboratory complete a comprehensive inventory of all hardware, software, and firmware as required by Army guidance; review all information technology research efforts for the potential Y2K impact; and review all contracts for inclusion of the Y2K contract provision. The Acting Deputy Assistant Secretary of the Army for Research and Technology concurred with the recommendations and stated that the Army Research Laboratory had taken or would take corrective actions.

Inspector General, DoD, Report No. 99-035, "Army Medical Research Institute of Infectious Diseases Preparation for the Year 2000," November 13, 1998. The report states that the Army Medical Research Institute of Infectious Diseases had not completed actions for Y2K issues to ensure that mission-essential systems would successfully operate after the turn of the century because it did not receive the draft Army Medical Command Y2K compliance guidance, compliance guidance for biomedical equipment, and facility infrastructure guidance until April 1998. As a result, the Institute could not ensure that information technology systems and ongoing research efforts would not have Y2K date-processing problems. The report recommended that the Army Medical Research Institute of Infectious Diseases complete the Y2K assessment of the biometric equipment and facility infrastructure inventories to include the following:

- adding research-specific computer hardware, software, and databases;
- developing cost plans to fix noncompliant Y2K systems and equipment;
- requesting funding assistance from the higher command;
- developing test plans for mission-essential systems and databases; and
- developing contingency plans for noncompliant hardware or software.

Additionally, the report recommended that the Army Medical Research Institute of Infectious Diseases document whether each research project was Y2K compliant and report the results through the Institute's Chief Information Officer. Finally, the report recommended that the Army Medical Research Institute of Infectious Diseases establish procedures requiring Institute personnel to notify the Army Medical Research Acquisition Activity of the need to include the Y2K clause in future contract efforts. The Deputy Assistant Secretary of the Army (Military Personnel Management and Equal Opportunity Policy) concurred with the recommendations and took action.

Inspector General, DoD, Report No. 99-034, "Management of the On-Site Inspection Agency Year 2000 Program," November 12, 1998. The report states that the On-Site Inspection Agency did not update its draft Y2K management plan to reflect the latest changes in the Draft DoD Management Plan. Also, it did not update the contingency plan for its mission-critical system and develop contingency plans for any other system the failure of which may cause disruption to the mission of the On-Site Inspection Agency. Additionally, the On-Site Inspection Agency did not:

- document the testing methodology for systems identified as Y2K compliant and
- include Y2K issues in its continuity-of-operations plans for the mission of the On-Site Inspection Agency.

Finally, the report states that the On-Site Inspection Agency did not take a proactive stance with regard to sector outreach. The report states that the On-Site Inspection Agency was not aware of the Sector Analysis, which assigns sectors of the Federal Government to lead Federal agencies to coordinate, plan, and lead the

execution of Y2K actions across all other agencies. As a result of the audit, the On-Site Inspection Agency started taking a proactive stance with regard to sector analysis.

The report recommended that the On-Site Inspection Agency implement the revisions from the DoD Management Plan, document changes in the status of systems, update the contingency plan for its mission-critical system and develop plans for any other system the failure of which might cause disruptions to its mission, document the testing methodology to show how systems are determined to be compliant, update the continuity-of-operations plan to address the Y2K issue, and continue taking a proactive stance with regard to sector outreach. The On-Site Inspection Agency concurred with all the recommendations, stating progress made and future intentions for each recommendation.

Inspector General, DoD, Report No. 99-031, "U.S. Pacific Command Year 2000 Issues," November 3, 1998. The review was conducted from June through August 1998. The report states that the U.S. Pacific Command needed to improve its Y2K program to minimize the adverse impact of Y2K date processing on its mission and on its mission-critical systems. Specifically, the report recommended that the U.S. Pacific Command include its reconciling and updating responsibility for the U.S. Pacific Command systems inventory in the U.S. Pacific Command Y2K Management Plan; establish offices of primary responsibility to monitor and track the status of supporting systems; modify the systems inventory to clearly identify critical Y2K data elements; develop system and operational contingency plans to establish alternate procedures to accomplish the mission; develop a complete inventory of all facility infrastructure systems and equipment and determine the overall responsibility for those items; and use selected command and joint exercises to test Y2K scenarios and contingency plans in an operational environment when possible. The U.S. Pacific Command concurred with the recommendations except to use selected command and joint exercises to test Y2K. However, the U.S. Pacific Command met the intent of the recommendation and stated that it would use separately developed operational evaluations and Joint Chiefs of Staff-directed Positive Response exercises to test the Y2K compliance and contingency planning.

Additionally, the audit reviewed the status of the U.S. Pacific Command Service component and sub-unified commands. The report states that the U.S. Pacific Command was increasing its awareness of its Service component and sub-unified commands. In May 1998, the U.S. Pacific Command requested its component and sub-unified commands, except the U.S. Special Operations Command Pacific, to provide Y2K status information. The report suggested the following:

- The U.S. Army Pacific Command was to identify the program offices that manage its systems, projected completion dates, and local points of contact for mission-critical systems.

- The U.S. Pacific Fleet Command was to raise its Y2K status to senior management within the U.S. Pacific Command, the Navy, and the DoD Chief Information Officer and Y2K Project Office.

- The Marine Forces Pacific Command was to establish Y2K focal points within all functional units and directorates to participate in the Y2K program and provide its Y2K inventory and its mission-critical systems to the U.S. Pacific Command and the Marine Corps.

- The U.S. Forces Japan was to complete an inventory, assess facility infrastructure systems and equipment, establish clear responsibility for those items, and develop contingency plans for the local area networks that it manages.

- The U.S. Forces Korea was to identify and concentrate on its mission-critical systems so that the appropriate executive agents were aware of the systems that were critical to U.S. Forces Korea; complete an inventory, assess facility infrastructure systems and equipment, and establish clear responsibility for those items; and inform the U.S. Pacific Command Y2K program office regularly on the status of its Y2K issues.

- The U.S. Special Operations Command Pacific was to continue to develop a complete inventory, identify its mission-critical systems, and report its Y2K status to the U.S. Special Operations Command and the U.S. Pacific Command.

- The Alaskan Command was to engage senior management to review the list of mission-critical systems; develop contingency plans for its mission-critical wide area network; complete an inventory and assess facility infrastructure systems and equipment; and determine the overall responsibility for those items.

Inspector General, DoD, Report No. 99-030, "Management of the Defense Technology Security Administration Year 2000 Program," November 3, 1998. The report states that the Defense Technology Security Administration did not classify systems as Y2K compliant only after completing Y2K compliance checklists; submit quarterly reports to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence); develop written contingency and continuity-of-operations plans; and take a proactive stance with regard to sector outreach. Further, unless the Defense Technology Security Administration made further progress on mitigating Y2K risks, the Defense Technology Security Administration, as part of the Defense Threat Reduction Agency, might not be able to fully execute its mission without undue disruptions. The report recommended that the Defense Technology Security Administration:

- report systems as compliant only after completing Y2K compliance checklists;

- submit quarterly reports to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in accordance with the latest DoD quarterly report guidance;

- develop, as appropriate, written contingency plans, in accordance with the DoD Management Plan and its revisions, for any system the failure of which may cause disruptions to the mission of the Defense Technology Security Administration;

• develop a continuity-of-operations plan, in accordance with the Draft DoD Management Plan, to minimize Y2K disruption to the mission of the Defense Technology Security Administration as a part of the mission of the Defense Threat Reduction Agency;

• assume a proactive stance with regard to sector outreach, both domestically and internationally; and

• implement the DoD Management Plan and its revisions and other DoD and Presidential Guidance.

The Defense Technology Security Administration concurred with the recommendations and stated that it had already developed a compliance checklist and was currently testing components.

Inspector General, DoD, Report No. 99-028, "Management of the Defense Special Weapons Agency Year 2000 Program," October 30, 1998. The report states that the Defense Special Weapons Agency recognized the importance of the Y2K issue and took positive actions to address the Y2K problem. However, the progress that the Defense Special Weapons Agency made in resolving its Y2K computing issue was not complete. The report recommended that the Defense Special Weapons Agency report systems as compliant only after completing Y2K testing and Y2K compliance checklists, develop contingency plans for its mission-critical systems and any other system of which its failure could cause disruption to the Defense Special Weapons Agency's mission, update the continuity-of-operations plan to specifically address the Y2K issue, assume a proactive stance with regard to sector outreach, and implement revisions to the DoD Y2K Management Plan and other DoD and Presidential guidance.

The Defense Special Weapons Agency concurred with recommendations. The Defense Special Weapons Agency stated that it would:

• review all systems currently reported as compliant and change the status of systems for which proper documentation did not exist,

• develop contingency plans for all mission-critical systems and update its continuity-of-operations plan to address Y2K issues,

• be proactive in regard to sector outreach, and

• implement the core ideas from the revisions to the DoD Management Plan that had survived at least one revision.

Inspector General, DoD, Report No. 99-027, "DoD Base Communications Systems Compliance With Year 2000 Requirements," October 30, 1998. The report states that of 275 telecommunications switches identified by DoD Components as non-Y2K compliant, 131 would not meet the Office of Management and Budget March 1999 deadline for implementation of all corrective actions to all systems. Additionally, none of the DoD Components that would not meet the deadline had contingency plans. As a result, DoD telecommunications capabilities could become unstable and unpredictable, the cumulative impact of non-Y2K compliant operational occurrences was expected to result in system failure, and DoD could miss available vendor discounts on

switch and software corrections if the required work was delayed. The report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) direct that Chief Information Officers in DoD Components prepare contingency plans for those switches that were not expected to be Y2K compliant by the Office of Management and Budget deadline of March 1999 and monitor progress on development of those contingency plans. The Senior Civilian Official of the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with the recommendation and stated that the switching problem was a high priority and, therefore, he was taking additional actions, including directing the Services to accelerate the switch implementation schedule.

Inspector General, DoD, Report No. 99-022, "Year 2000 Conversion at the Army Major Range and Test Facilities," October 29, 1998. The report states that the three Army major range and test facilities visited, the Aberdeen Proving Ground, the White Sands Missile Range, and the Yuma Proving Ground, were on schedule to complete the renovation phase by September 1998. All required documentation and certification forms for the compliant systems were completed as required by the Army Action Plan and the DoD Management Plan. The report contains no findings or recommendations.

Inspector General, DoD, Report No. 99-017, "Year 2000 Conversion of the Airborne Warning and Control System," October 19, 1998. The report states that the Airborne Warning and Control System program office did not modify all existing contracts to comply with the Federal Acquisition Regulations (48 Code of Federal Regulations Parts 39.002 and 39.106) that address Y2K compliance definitions and language. The report states that program officials acted promptly and responsibly when the condition was brought to the attention of the program office. Additionally, the contingency plans did not:

- contain all of the Airborne Warning and Control System mission-critical and mission-essential systems that process dates;
- identify specific actions to take during and after a Y2K failure; and
- address several potential Y2K scenarios.

The reports states that the program office took immediate action to make the necessary changes. The report states that the audit reviewed the revised contingency plans and determined the action taken to be satisfactory.

Overall, the report states that the Airborne Warning and Control System program office took an aggressive and proactive approach on the issues under its purview to ensure that the Airborne Warning and Control System continuity-of-operations was not disrupted by Y2K-related issues. Program office managers successfully planned, executed, and coordinated their Y2K efforts with key organizations that support the Airborne Warning and Control System to ensure a smooth transition into the Y2K. As a result, Y2K-related issues were not expected to disrupt Airborne Warning and Control System missions, provided that the operations and support infrastructure of the 552nd Air Control Wing and Air Force Air Logistics Centers was Y2K compliant. The report made no recommendations.

Inspector General, DoD, Report No. 99-015, "Joint Centers' Year 2000 Issues," October 16, 1998. The report states that the Joint Centers did not address all potential Y2K problems. Generally, the Joint Centers did not assess all mission-critical systems for Y2K compliance status, adequately certify and document mission-critical systems as Y2K compliant, develop contingency plans, and coordinate Y2K efforts with the U.S. Atlantic Command and the Joint Staff. The Joint Battle Center had a commendable Y2K program in place, but the Joint Command and Control Warfare Center, the Joint Communications Support Element, the Joint Warfare Analysis Center, and the Joint Warfighting Center needed to take immediate action to comply with Joint Staff and DoD guidance. The report concludes that unless Y2K risks were mitigated, four of the five Joint Centers might not be able to fully execute their missions. Further, the Joint Centers might not be able to effectively facilitate or participate in joint exercises that would test Y2K scenarios in an operational environment.

The report recommended that the Joint Command and Control Warfare Center, the Joint Communications Support Element, the Joint Warfare Analysis Center, and the Joint Warfighting Center take immediate action to complete assessments for determining the Y2K compliance status of all mission-critical systems, certify and document all internally managed compliant systems, and develop contingency plans for all mission-critical systems that were not scheduled to be compliant by December 31, 1998.

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

Inspector General, DoD, Report No. 99-003, "Air Force Research Laboratory Preparation for Year 2000," October 5, 1998. The report states that the Air Force Research Laboratory had established a process for determining whether the laboratory had a potential Y2K impact and was actively determining its systems' vulnerability to the date-processing problem. However, the Air Force Research Laboratory had not met the required time frames for the Air Force Materiel Command Y2K Program Management Plan for identifying and resolving any Y2K impact for infrastructure items. The Air Force Research Laboratory officials emphasized the importance of identifying and resolving potential Y2K problems, began conducting a comprehensive inventory of information technology systems, began reviewing ongoing research efforts for Y2K concerns, and modified contracts for Y2K compliance, where applicable. The report concludes that although the Air Force Research Laboratory was somewhat behind overall DoD schedule guidelines for the infrastructure items, an effective effort was under way for minimizing any Y2K date-processing problems. The report contains no recommendations.

Inspector General, DoD, Report No. 98-218, "Major Range and Test Facility Base Year 2000 Initiatives at the Naval Air Warfare Center-Aircraft and Weapons Divisions, and the Atlantic Undersea Test and Evaluation Center," September 30, 1998. The report states that, for the 30 systems reviewed, Navy officials from the Major Range and Test Facility Base at the Naval Air Warfare Center-Aircraft and Weapons Divisions and the Atlantic Undersea Test and Evaluation Center had initiated positive actions to resolve and accurately report on date-processing issues for potential Y2K-related failures that could affect the

test and evaluation activities of the Navy. The audit identified to a Navy official that the Navy did not completely assess the subsystems for two of the systems. Upon identification, the Aircraft Division moved its large area tracking range, which contained seven subsystems, from the renovation phase back to the assessment phase. In addition, the Naval Air Warfare Center officials at the Weapons Division, China Lake, moved the slate range facility system, which contained 10 subsystems, from the validation phase to the assessment phase. Also, officials at the Naval Air Warfare Center-Weapons Division, Point Mugu, implemented several actions that would improve the coordination and standardization process for making all weapons division systems Y2K compliant. As a result, resolution of and reporting on the Y2K progress for Major Range and Test Facility Base test and evaluation systems at the Naval Air Warfare Center-Aircraft and Weapons Divisions were improving. The report made no recommendations.

Inspector General, DoD, Report No. 98-203, "Naval Research Laboratory Preparation for Year 2000," September 23, 1998. The report states that the Naval Research Laboratory did not develop a comprehensive Y2K activity plan, develop a complete inventory of information technology systems, examine ongoing research efforts for a potential Y2K impact, and modify contracts to ensure receipt of Y2K compliant systems. The Naval Research Laboratory did not accomplish those actions because it did not fully comply with the Navy Y2K guidance.

The Naval Research Laboratory officials stated that the Navy organizations were allowed flexibility in using the Navy Action Plan to meet individual needs of the organization, and Navy organizations were not required to follow the Navy Action Plan. Further, the Commander, Naval Research Laboratory, stated that he was satisfied with the approach that the Naval Research Laboratory Y2K officials were taking and that he would certify that systems used and the associated interfaces would not be affected by transitioning to the Y2K. The report concludes that if the Naval Research Laboratory did not take actions outlined in the report, it could not adequately identify and minimize potential Y2K problems.

The report recommended that the Naval Research Laboratory develop an activity plan to include all areas of laboratory based on the Navy Action Plan guidance; develop a complete inventory list of all Naval Research Laboratory hardware, software, and firmware, including purchases with credit cards and delivery orders; develop test, contingency, and cost plans as required by the Navy Action Plan guidance; review all information technology research efforts for potential Y2K impacts and initiate the necessary corrective actions; and review all existing contracts or other acquisition instruments for information technology and modify contracts for the Y2K compliance requirement, where appropriate. The Office of the Assistant Secretary of the Navy (Research, Development, and Acquisition) concurred with the recommendations and provided the actions that the Naval Research Laboratory completed and dates for actions that the Naval Research Laboratory would complete.

Inspector General, DoD, Report No. 98-207, "Year 2000 Contract Language for Weapon Systems," September 22, 1998. The report states that of the 16 weapon systems reviewed, 9 weapon systems had contracts that did not contain language from Federal Acquisition Regulation 39.106, "Year 2000 Compliance." However, the report states that at the time of the audit, the Under Secretary of Defense for Acquisition and Technology had not issued Y2K guidance for weapon systems. On August 7, 1998, the Secretary of Defense directed the Services and Defense agencies to report on each major acquisition system under their purview. Each report was to address areas of Y2K compliance or noncompliance for each system. The Secretary of Defense also directed that funds not be obligated for any contract for information technology or national security systems that process date-related information when that contract did not contain Y2K requirements specified in Section 39.106 of the Federal Acquisition Regulation. During the audits of the weapon systems, the Program Management Offices initiated action to ensure that the contracts and solicitations for the nine weapon systems would include Y2K compliance language.

The report concludes that the action taken by the Program Management Offices should have helped DoD in its efforts to ensure that no system would be adversely affected by Y2K problems, and the actions taken by the Secretary of Defense should have corrected the problems identified. Therefore, the report made no recommendations.

Inspector General, DoD, Report No. 98-196, "Navy Special Access Program Community Preparation for Year 2000 Compliance," August 28, 1998. The report states that the Navy Special Access Program Central Coordinating Office provided adequate oversight to Navy special access programs for Y2K compliance since the November 4, 1997, memorandum from the Director, Special Access Program Coordination Office, DoD. Since the memorandum, the Navy Special Access Program Central Coordinating Office established a Y2K point of contact to coordinate Y2K information for all Navy special access programs, established a Y2K website on the Navy special access program internal-security intranet to disseminate information from the Department of the Navy Chief Information Officer's Y2K website to the Navy special access programs, and began requiring quarterly reports from Navy special access programs on their Y2K status. Four of the five selected Navy special access programs assessed their systems for Y2K compliance; identified interfacing systems; and, where appropriate, started modifying contracts to include Y2K compliance. The fifth Navy special access program had begun assessing and solving Y2K compliance issues in November 1995. The report contained no recommendations.

Inspector General, DoD, Report No. 98-194, "U.S. Atlantic Command Year 2000 Issues," August 27, 1998. The review was conducted from April through June 1998. The report states that the U.S. Atlantic Command needed to do more in gaining visibility over its mission-critical systems owned by the Services and Defense agencies, reconciling its managed-systems inventory, preparing compliance checklists and certifying U.S. Atlantic Command-managed systems as compliant, establishing directorate responsibility for all of its commercial off-the-shelf products, developing system and operational contingency plans to establish alternate procedures to accomplish the mission, and using selected command and joint exercises to test Y2K scenarios and contingency plans in an operational environment when possible.

The report recommended that the U.S. Atlantic Command establish procedures and time frames for the offices of primary responsibility to:

- monitor and track the status of mission-critical systems that the Services and Defense agencies own,

- join with functional counterparts at other unified commands to obtain the status of mission-critical systems from the Services and Defense agencies, and

- report the status of those systems to the U.S. Atlantic Command Y2K program office.

Additionally, the report recommended that the U.S. Atlantic Command complete the reconciliation of the managed-systems inventory, clearly define reportable systems and how reportable systems should be categorized, complete certification checklists to fully support systems as Y2K compliant, establish offices of primary responsibility for nonstandard commercial off-the-shelf products, complete the reconciliation of compliance discrepancies, develop system and operational contingency plans, and use selected command and joint exercises to test Y2K scenarios and contingency plans in an operational environment when possible.

The U.S. Atlantic Command's comments were responsive. The U.S. Atlantic Command stated that it developed a database to monitor and track the status of mission-critical systems that the Services and Defense agencies own. The offices of primary responsibility were to report all information on supporting systems and commercial off-the-shelf software to the U.S. Atlantic Command Y2K program office on a monthly basis. Additionally, the U.S. Atlantic Command stated that it completed the managed-inventory reconciliation, established completion dates for all certification compliance checklists and contingency plans, established offices of primary responsibility for all commercial off-the-shelf products, and was providing input to the Joint Staff for the Chairman of the Joint Chiefs of Staff operation evaluation plan.

Inspector General, DoD, Report No. 98-193, "Evaluation of the Defense Megacenters Year 2000 Program," August 25, 1998. The report states that although much progress had been made in converting the Defense Megacenters' systems to Y2K compliance, problems remained in three areas: reporting, testing, and contingency planning.

Reporting. The report states that the Defense Information Systems Agency Western Hemisphere Y2K status reports for executive software were incomplete and could be misinterpreted. The Y2K status reports did not reasonably state the amount of conversion work to be done and did not provide visibility of the issues blocking progress. The reports showed that the executive software product inventory was 60 percent compliant but did not show that the domain compliance was zero percent. The status reports concentrated on the availability of Y2K compliant products rather than the status of replacing the noncompliant products in each production domain. The Defense Information Systems Agency Western Hemisphere and the Central Design Activities, part of the Military Departments and Defense agencies, had joint responsibility for fixing segments of the domains. However, the two had not coordinated their efforts in

either solving or reporting their Y2K problems. As a result, DoD was at risk of classifying mission-critical systems on mainframe computers as being Y2K compliant when they were not.

The report recommended that the DoD Chief Information Officer direct the Central Design Activities to expedite the establishment of written agreements with the Defense Megacenters and the Systems Support Office for domain executive software Y2K renovation. Additionally, the report recommended that the DoD Chief Information Officer advise the Secretaries of the Military Departments and the Defense agencies when Defense Megacenters identify domains that have high risk of Y2K noncompliance. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with the recommendation and stated that on July 2, 1998, the Deputy Secretary of Defense directed written agreements between the Defense Information Systems Agency and domain users. In addition, the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) coordinated a Secretary of Defense memorandum that stated funds were not to be obligated for any domain user that failed to sign explicit test agreements with the Defense Information Systems Agency by October 1, 1998. The memorandum, dated August 7, 1998, also states that the Defense Information Systems Agency was to provide a report to the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) by October 15, 1998, listing all domain users that failed to sign test agreements with the Defense Information Systems Agency by October 1, 1998. Finally, the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that it would request that the Y2K compliance reports from the Defense Information Systems Agency include items that would identify domains, mission-critical systems, or national security systems that had a high risk of Y2K noncompliance.

The report also recommended that the Defense Information Systems Agency direct the Defense Megacenters and the Systems Support Office to establish written agreements with the Central Design Activities and Defense Megacenters and report complete Y2K status and applications that were affected by domain for inclusion in Defense Information Systems Agency Western Hemisphere reports to Defense Information Systems Agency Headquarters. The report was to include a status of the coordinated agreements and schedules with the Central Design Activities. Additionally, the report recommended that the Defense Information Systems Agency report the domain Y2K compliance status to the Office of the Secretary of Defense. The Defense Information Systems Agency concurred with the recommendations and stated that it would establish agreements by September 18, 1998; report Y2K status by domain and the affected applications by August 17, 1998; and report domain Y2K compliance status to the Office of the Secretary of Defense by August 21, 1998.

Testing. The report states that the Defense Information Systems Agency Western Hemisphere did not plan to test the non-Standard Operating Environment, computer hardware, and facility equipment for Y2K compliance. As a result, mission-critical processing could have been at risk of date-related failures.

The report recommended that the Defense Information Systems Agency direct the Defense Megacenters and the Systems Support Office to plan, conduct, and provide progress reports for comprehensive Y2K testing on nonstandard executive software, computer hardware, and facility equipment. The Defense Information Systems Agency concurred, stating that it intends to selectively test components of the nonstandard executive software, computer hardware, and facility equipment for Y2K compliance. Because of time and resource constraints, the Defense Information Systems Agency would not be able to test all of the executive software, but at the time it was meeting with customers to jointly decide the products that would be tested. The estimated completion date was December 31, 1998.

Planning. The report states that the Defense Information Systems Agency recognized the need for contingency plans and issued guidance directing the Defense Megacenters to write specific contingency plans. However, the guidance did not impose milestones for when the individual Defense Megacenters should have the action plans written. Further, the report states that the Defense Information Systems Agency needed to expand on the contingency planning guidance for recovering from Y2K failures of executive software, computer hardware, and facilities equipment. Without more comprehensive planning, mission-critical systems may not be able to continue operations if Y2K failures occur.

The report recommended that the Defense Information Systems Agency direct the Defense Megacenters to conduct contingency planning and that the requirements be issued to the Defense Megacenters. The direction was to include writing requirements to:

- complete risk assessments;
- plan for contingency coverage of executive software, computer hardware, and facilities equipment;
- establish contingency planning milestones; and
- report the status of contingency planning development and contingency plan validation.

The Defense Information Systems Agency concurred and stated that it would instruct the Defense Megacenters to conduct contingency planning and issue requirements addressed in the recommendation. The estimated completion date was November 2, 1998.

Inspector General, DoD, Report No. 98-188, "U.S. Space Command Year 2000 Issues," August 18, 1998. The review was conducted from February through April 1998. The report states that the U.S. Space Command and component commands had taken actions to address the Y2K problem, but did not complete all the actions necessary to minimize the adverse impact of Y2K date processing on its mission and its mission-critical systems.

The report recommended that the U.S. Space Command identify Y2K as a readiness issue and include functional directorates in future warfighter Y2K conferences that the Joint Staff hosts. The report also recommended that the U.S. Space Command develop the following:

- a written Y2K management plan,
- a complete list of mission-critical systems,
- contingency plans for mission-critical systems that the U.S. Space Command manages,
- operational contingency plans for mission areas, and
- comprehensive and complete test plans.

Additionally, the report recommended that the U.S. Space Command complete the identification of interfaces and prepare written interface agreements for mission-critical systems that the U.S. Space Command manages, coordinate Y2K solutions and contingency plans with its component commands, and use selected command and joint exercises to test Y2K scenarios and contingency plans in an operational environment when possible. The report recommended that the Joint Staff include all functional directorates and component commands in the warfighter Y2K conference. The U.S. Space Command and the Joint Staff concurred with the recommendations of the report. The U.S. Space Command stated that it initiated action to address the recommendations of the report. The Joint Staff stated that all functional directorates would be invited to the Joint Staff's August 1998 and following Y2K conferences.

Inspector General, DoD, Report No. 98-187, "Year 2000 Computing Problem at Air Force Major Range and Test Facilities," August 14, 1998. The report states that two of the four Air Force major range and test facilities visited were behind schedule in assessing range business and test information systems to determine the systems that need to be upgraded or replaced to ensure Y2K compliance. Arnold Air Force Base and Eglin Air Force Base had identified the systems and were on schedule to meet the Air Force renovation phase milestone completion date of June 30, 1998. However, Edwards Air Force Base and Nellis Air Force Base were still in the awareness and assessment phases and might not meet the renovation milestone date. In addition, the ranges identified certain systems as mission critical that might need a higher funding priority to ensure Y2K compliance. The report concludes that if the Air Force systems fail to recognize January 1, 2000, critical warfighting functions such as combat, communications, surveillance, and air traffic control functions could be seriously affected. Furthermore, delays in supply shipments, errors with personnel-related information, and unreliable budget estimates could occur.

The report recommended that the Air Force Test and Evaluation Directorate and the Air Force Operations and Training Directorate review the status of the Y2K problem at the major range and test facilities to ensure that system assessment, repair, replacement, and testing were completed by December 1999. The Air Force Test and Evaluation Directorate agreed with the recommendation and stated that it would track the progress of the ranges and make every effort to ensure that the Air Force range and test facilities comply with the DoD

Management Plan. The comments included updated information and a list of corrective actions accomplished and to be accomplished. Additionally, the Acting Deputy Secretary of Defense (Chief Information Officer Policy and Implementation) stated that the Air Force should accelerate its schedule to achieve compliance by December 1998 because those ranges and facilities may be required to test other systems for Y2K compliance.

Inspector General, DoD, Report No. 98-184, "Management of the Defense Information Systems Agency Year 2000 Program," August 4, 1998. The review was conducted from October 1997 through March 1998. The report states that the Defense Information Systems Agency needed to address several critical factors to be in compliance with the DoD Management Plan. Specifically, the Defense Information Systems Agency needed to:

- update the Defense Information Systems Agency Y2K Problem Management Plan to include the requirements of the DoD Management Plan;

- disseminate the DoD Management Plan, the Defense Information Systems Agency Y2K Problem Management Plan, and other guidance in entirety to the operating levels;

- accurately report and document Defense Information Systems Agency Y2K status as prescribed in the exit criteria within the DoD Management Plan;

- identify all interfaces and assign risks and efforts to resolve Y2K problems for document agreements with interface partners on how the interfaces should be made Y2K compliant;

- prepare updated Y2K cost estimates for each system to determine whether additional funding was needed;

- develop contingency plans for mission-critical systems in accordance with the DoD Management Plan and communicate the plans to interface partners; and

- validate systems as Y2K compliant only after fully documenting test results using the official compliance checklists.

The report recommended that the Defense Information Systems Agency update the management plan to incorporate the changes to the extent of the guidance documented within the DoD Management Plan, disseminate guidance to the operating level, follow exit criteria prescribed in the DoD Management Plan to accurately document the reported progress for Y2K, identify all interfaces to resolve any problems and communicate the resolutions to all interface partners, provide cost estimates for each system, develop contingency plans for systems that would not complete the revised implementation phase schedule for December 1998, and determine system Y2K compliance status only after the system had been tested and certified as compliant.

The Defense Information Systems Agency generally concurred with the recommendations and stated corrective actions to be taken. However, the Defense Information Systems Agency stated that DoD agreed to exempt communications transport systems from developing formal interface agreements because adherence

to applicable international and national standards would accomplish the same results. The report states that the audit could not verify the exemption. The Draft DoD Management Plan does not provide such an exemption, and the staff in the Office of Year 2000 Oversight and Contingency Planning was not aware of any plans to include such a provision. The report requested that the Defense Information Systems Agency clarify the requirements for establishing interface agreements for telecommunications transport systems with DoD Y2K officials and provide comments on that aspect of the report, including any estimated completion dates for any planned actions.

Inspector General, DoD, Report No. 98-182, "Year 2000 Program at the Defense Advanced Research Projects Agency," July 31, 1998. The report states that the Defense Advanced Research Projects Agency properly examined its internal management information systems for Y2K compliance; however, it did not review research contracts for prototypes for Y2K considerations. As a result, the Defense Advanced Research Projects Agency could not ensure that research projects would not have Y2K date-processing problems. The report recommended that the Defense Advanced Research Projects Agency review research efforts, including any planned system interfaces necessary for research efforts, to determine whether they had a potential Y2K impact and add, when appropriate, the Y2K compliance language to the contracts identified. Additionally, the report recommended that the Defense Advanced Research Projects Agency review contracts for Y2K compliance as part of the self-evaluation process for the management control program. The Defense Advanced Research Projects Agency generally concurred with the recommendations, stating that it would address Y2K vulnerabilities on contracted efforts of experimental prototype systems and add Y2K compliance language wherever appropriate. Further, the Defense Advanced Research Projects Agency stated that it would conduct the reviews of contracts and would make the reviews a part of the management control program's self-evaluation process.

Inspector General, DoD, Report No. 98-180, "Ballistic Missile Defense Organization Year 2000 Initiatives," July 16, 1998. The report states that officials from the Medium Extended Air Defense System program office and the National Missile Defense program office, both sponsored by the Ballistic Missile Defense Organization, initiated positive action to ensure that future contracts for programs would include Y2K-compliance clauses. Program officials changed the information to be provided to current contractors, and Ballistic Missile Defense Organization officials planned to revise the lead system integrator contract after the audit identified the omission of Y2K compliance language in the solicitations sent to prospective bidders. Because management took corrective action during the audit, the report made no recommendations concerning Y2K compliance clauses.

The report also states that the Ballistic Missile Defense Organization's Y2K quarterly report, April 1998, did not accurately report the Ballistic Missile Defense Organization's progress in solving the Y2K problem for the Theater High-Altitude Area Defense program. In addition, the Ballistic Missile Defense Organization incorrectly approved the Theater High-Altitude Area Defense and the National Missile Defense programs to exit the assessment phase because it did not verify whether the programs met the requirements of the assessment phase. The report recommended that the Ballistic Missile Defense Organization review the Y2K effort for the Theater High-Altitude Area Defense program and

determine whether it meets the exit criteria for the assessment phase; determine the correct reporting phase for the next DoD Y2K quarterly report; and implement procedures to certify that the exit criteria are met for each mission-critical program before granting approval for it to proceed to the next Y2K phase. In addition, the report recommended that the Ballistic Missile Defense Organization require the National Missile Defense program office to obtain a detailed assessment plan from each program element. The Ballistic Missile Defense Organization took actions meeting the intent of the recommendations.

Inspector General, DoD, Report No. 98-173, "U.S. Central Command Year 2000 Issues," July 2, 1998. The report states that the U.S. Central Command took several positive actions to address its Y2K problem. However, the U.S. Central Command and the Joint Staff had not completed all of the actions necessary to minimize the adverse impact of Y2K date processing in mission and mission-support systems.

The report recommended that the U.S. Central Command monitor and implement DoD Management Plan revisions, complete the identification of mission-critical supporting systems and system interfaces, research Y2K compliance of vendor software and test mission-critical vendor software, prepare written interface agreements, develop contingency plans for U.S. Central Command mission-critical managed and supporting systems and develop operational contingency plans as needed, document test plans and certify the level of Y2K compliance for managed systems, coordinate Y2K solutions with the Component Commands, and use selected command and joint exercises to test Y2K scenarios in an operational environment. The U.S. Central Command concurred with the recommendations of the report.

The report also recommended that the Joint Staff develop a composite DoD mission-critical database and assist the unified commands in obtaining Y2K information on mission-critical supporting systems that Services or other organizations manage, implement procedures to monitor and track the status of mission-critical supporting systems, assist the unified commands in testing systems and applications common to the unified commands, disseminate Y2K information on commercial off-the-shelf products, and use selected joint exercises to test Y2K scenarios in an operational environment. The Joint Staff concurred with the recommendations of the report.

In an effort to provide assistance to the unified commands, the Joint Staff extracted data from the database developed by the DoD Y2K Project Office and posted it to the Joint Staff Y2K web site. The database was not available on-line because of classification issues. The Joint Staff also stated that it had been facilitating the Joint Interoperability Test Command for Y2K testing of systems owned by the unified commands. Finally, the Joint Staff stated that it was developing a Y2K operational evaluation plan for use by the unified commands and the Services during exercises and other opportunities from now until the Y2K. In June 1998, the Vice Chairman, Joint Chiefs of Staff, sent a message to the unified commands, the Services, and the Defense agencies. The message provided a synopsis of the operational evaluation plan, solicited unified command involvement in the Y2K process, and requested feedback on Y2K operational evaluation opportunities.

Inspector General, DoD, Report No. 98-169, "DoD Year 2000 Computing Problem Reports: Lessons Learned From the Defense Integration Support Tools Database," June 29, 1998. The report states that DoD had no viable repository of Y2K information that DoD managers could use for tracking, reporting, monitoring, and overseeing DoD Y2K compliance efforts. Previously, DoD used the Defense Integration Support Tools database as the official repository of DoD Y2K information, but then DoD discontinued it for Y2K use. Further, DoD managers were unable to rely on the Defense Integration Support Tools database for reporting and oversight purposes. Consequently, DoD managers did not have a DoD-wide automated mechanism for Y2K reporting and oversight purposes. The report states that the DoD Chief Information Officer had taken action to develop a new database tool to replace the Defense Integration Support Tools database for Y2K use. However, the new database could also encounter data unreliability unless DoD applied the lessons learned from the Defense Integration Support Tools database.

The report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) immediately implement a replacement database for the Defense Integration Support Tools database to track, monitor, report, and oversee DoD Y2K efforts. Additionally, the report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) apply lessons learned from the Defense Integration Support Tools database to the replacement database. Specifically, the replacement database was to:

- provide reliable information for tracking, monitoring, reporting, and overseeing DoD Y2K efforts;

- provide adequate management controls for data entry to affix responsibility for accuracy at the DoD Component Y2K designated office level;

- allow for flexibility to accommodate changes in Office of Management and Budget reporting requirements;

- be compatible with DoD Component internal databases for effective importing of data; and

- allow for appropriate menu choices to eliminate blank fields.

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with all recommendations and stated that the office had developed a replacement database to track, monitor, and report DoD Y2K efforts at a high level. The Assistant Secretary also described several initial actions already taken to implement the replacement database and to preclude recognized operational weaknesses associated with the Defense Integration Support Tools database. The DoD Y2K Oversight and Contingency Planning Office had since posted the DoD Y2K database to the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) web page. However, the database was removed from the web page in September 1998.

The Deputy Assistant Secretary of Defense for Policy and Implementation placed the new DoD Y2K database on hold because of data discrepancies and inaccuracies. The data call for the Quarterly Office of Management and Budget

Report commanded greater confidence in the accuracy of the data than DoD Components were providing. As a result, the Deputy Assistant Secretary of Defense for Policy and Implementation initiated a Y2K Database Task Force to synchronize the data. The Deputy Assistant Secretary of Defense for Policy and Implementation considered the data too sensitive to be on the web but stated that it could remain on the Non-Secure Internet Protocol Router Network with controls. The Carnegie-Mellon University developed a secure middleware software package for security extranet to control access.

Inspector General, DoD, Report No. 98-147, "Year 2000 Certification of Mission-Critical DoD Information Technology Systems," June 5, 1998. The report estimated that DoD Components certified only 109 (25.3 percent) of the 430 systems reported as Y2K compliant in November 1997. Systems were not certified because DoD Components did not adequately implement and enforce the guidance in the DoD Management Plan or their own Y2K guidance. Additionally, the report stated that the initial DoD Management Plan was not consistently clear as to specific Y2K certification requirements. As a result, mission-critical DoD information technology systems could unexpectedly fail because they were classified as Y2K compliant without adequate verification and validation.

The report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issue to DoD Components clarified DoD Y2K certification requirements and issue to DoD clear, firm Y2K quarterly reporting requirements. Additionally, the report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) develop guidance for the signature of the Deputy Secretary of Defense that directs DoD Components to establish oversight processes and procedures to effectively enforce those DoD requirements.

The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with the recommendations and stated that it instituted several measures, including the following:

- introducing the requirement for all mission-critical systems to have independent tests and operational contingency plans,

- updating the DoD Management Plan in June 1998 with guidance on certification and testing, and

- developing a new Y2K database that would forecast the target date to complete each phase of Y2K remediation for each mission-critical system. DoD was to report the progress against the benchmarks to the Office of Management and Budget on the tenth day of each month.

The Draft DoD Management Plan revised the requirements on compliance certification. The Draft DoD Management Plan is specific and states that each system is certified when it receives a signature by the system manager, the project manager, and the customer on the checklist confirming that testing in accordance with the Draft DoD Management Plan was completed and the results indicated that the system is compliant.

On August 7, 1998, the Secretary of Defense issued a memorandum, "Year 2000 Compliance," requiring the Services and Defense agencies to report to the Secretary of Defense every Acquisition Category I, Acquisition Category IA, and Acquisition Category II system within its purview. Further, each report was to address Y2K compliance or areas of noncompliance of each respective system. Additionally, the memorandum requires Military Departments, Commanders in Chief, and Defense agencies to accurately report their list of mission-critical systems in the DoD Y2K database.

On August 24, 1998, the Deputy Secretary of Defense issued a memorandum, "Year 2000 (Y2K) Verification of National Security Capabilities," requiring the Chief of Staff of the Army, the Chief of Naval Operations, the Chief of Staff of the Air Force, the Commandant of the Marine Corps, and the Directors of the Defense Agencies to certify by November 1, 1998, that they had tested information technology and national security system Y2K capabilities of their respective component's systems in accordance with the DoD Management Plan. Each certification was to cite all mission-critical systems that were yet to be validated as Y2K compliant along with a timeline for expected validation of the systems.

Inspector General, DoD, Report No. 98-129, "U.S. Special Operations Command Year 2000 Issues," May 8, 1998. The report states that the progress that the U.S. Special Operations Command made in resolving its Y2K problem was not complete. To ensure that its mission-critical systems would successfully operate at the Y2K and beyond, the U.S. Special Operations Command, including its component commands and functional directorates, was to address several critical issues. Unless the U.S. Special Operations Command made further progress, it faced a high risk that Y2K-related disruptions would impair its mission capabilities.

The report recommended that the U.S. Special Operations Command implement revisions to the DoD Management Plan, continue to identify mission-critical systems that the U.S. Special Operations Command managed and the associated interfaces for those systems, prepare written interface agreements and contingency plans, continue to identify mission-critical supporting systems that Services or other organizations manage, refine cost estimates for each individual system to determine amounts needed for fund allocation, determine systems as Y2K compliant only after testing the systems and completing compliance checklists, and use selected command and joint exercises to test Y2K scenarios in an operational environment. Additionally, the report recommended that the Joint Staff assist the unified commands in obtaining Y2K information on mission-critical supporting systems that Services or other organizations manage, assist the unified commands in testing systems and applications that are common to the unified commands, and use selected joint exercises to test Y2K scenarios in an operational environment. The U.S. Special Operations Command and the Joint Staff concurred with the recommendations of the report, stating progress made and future intentions for each recommendation.

Inspector General, DoD, Report No. 98-112, "Year 2000 Reporting for Defense Finance and Accounting Service Cleveland Center Systems," April 17, 1998. The report states that information on the Defense Finance and Accounting Service Cleveland Center systems, as reported in the Defense Integration Support Tools database, was not complete, accurate, and consistent with the Defense Finance and Accounting Service Cleveland Center quarterly reports. The Defense Finance and Accounting Service Cleveland Center did not enter all required data elements into the Defense Integration Support Tools database for each system and verify that system information reported in the Defense Integration Support Tools database was consistent with the Defense Finance and Accounting Service Cleveland Center quarterly reports. As a result, the Defense Integration Support Tools database was unreliable for making decisions about Y2K issues. The report concludes that the lack of data integrity could increase the potential for system failures because internal and external users relied on the information reported, regardless of the database that was used as the repository.

Because the Defense Finance and Accounting Service actions were responsive to suggestions made during the review of the Defense Integration Support Tools database, the report contains no recommendations. The Defense Finance and Accounting Service agreed with the issues identified and developed the following three-phase plan:

- The Defense Finance and Accounting Service would perform a complete review of all systems registered in the Defense Integration Support Tools database.

- The Defense Finance and Accounting Service centers responsible for the systems would identify and supply the missing data in the Defense Integration Support Tools database.

- The Defense Finance and Accounting Service would gather the missing data and work with the Defense Integration Support Tools database Help Desk to enter the information into the Defense Integration Support Tools database.

The Defense Finance and Accounting Service stated that it would accomplish the corrective actions in February and March 1998. However, on February 4, 1998, the DoD Chief Information Officer issued a memorandum classifying the Defense Integration Support Tools database as secret. The decision was based on a National Security Agency review that determined that the vulnerability of the information in the Defense Integration Support Tools database was a threat to national security. On March 20, 1998, the DoD Chief Information Officer decided that DoD would no longer use the Defense Integration Support Tools database.

Inspector General, DoD, Report No. 98-111, "Year 2000 Initiatives at the Defense Finance and Accounting Service Cleveland Center," April 16, 1998. The report identifies issues at the Defense Finance and Accounting Service Cleveland Center. Specifically, the Defense Finance and Accounting Service Cleveland Center did not accurately report Y2K progress and did not effectively complete all necessary interface agreements.

Defense Finance and Accounting Service Reporting Requirements. The report states that the Defense Finance and Accounting Service Cleveland Center's quarterly reports on Y2K were unreliable and did not accurately report the progress in solving Y2K problems at the Defense Finance and Accounting Service Cleveland Center. Specifically, the Defense Finance and Accounting Service Cleveland Center did not perform adequate assessments of systems reported in the renovation phase and did not meet all requirements for making systems Y2K compliant. The quarterly reports were unreliable because the Defense Finance and Accounting Service Cleveland Center did not implement the requirements of the DoD Management Plan, which specifies the exit criteria and minimum requirements for a system-level Y2K project plan. As a result, DoD and Defense Finance and Accounting Service management were relying on inaccurate information, which increased the risk of system failures because of Y2K noncompliance.

The report recommended that the Defense Finance and Accounting Service Cleveland Center direct its system managers to:

- fulfill the assessment phase exit criteria in the DoD Management Plan for systems reported as being in the renovation phase and

- meet all criteria in the DoD Management Plan for systems listed as Y2K compliant, including completion of the Defense Finance and Accounting Service compliance certification checklist, before reporting systems as compliant.

Additionally, the report recommended that the Defense Finance and Accounting Service Cleveland Center establish a verification mechanism to ensure that systems are progressing as needed to meet the deadline and that information reported to DoD and Defense Finance and Accounting Service management is accurate, is reliable, and reflects the status of each Defense Finance and Accounting Service system. The Defense Finance and Accounting Service concurred, stating that the managers would be directed to take the necessary actions for the assessment phase and certification of systems. Additionally, the Defense Finance and Accounting Service Cleveland Center will conduct monthly Y2K Control Board meetings to provide a mechanism for monitoring system progress and ensuring corrective actions should problems arise.

Interface Agreements. Additionally, the report states that the Defense Finance and Accounting Service Cleveland Center had not effectively completed all necessary interface agreements. Of the 152 interface agreements required for the 9 Defense Finance and Accounting Service Cleveland Center systems reviewed, 73 interface agreements for 3 systems had not been established. Of the remaining 79 interface agreements that were established:

- 54 did not identify strategies and changed record formats,

- 53 lacked milestone dates for implementation,

- 51 did not identify test files, and

- 62 did not identify a point of contact.

The Defense Finance and Accounting Service Cleveland Center did not have a verification process to ensure that adequate interface agreements were in place.

The report recommended that the Defense Finance and Accounting Service Cleveland Center establish milestones for verification and perform the verification process to ensure that all interface agreements are complete and include the necessary elements. The Defense Finance and Accounting Service concurred, stating that the Defense Finance and Accounting Service Cleveland Center established a milestone of March 31, 1998, to correct deficiencies identified with Y2K interface agreements and that system managers would verify that existing interface agreements include the necessary elements.

Inspector General, DoD, Report No. 98-077, "Year 2000 Computing Problem Reports: August 1997 Report," February 18, 1998. The report states that the DoD Component second quarter reports on the Y2K issue did not provide all the required information and were not fully reliable. Accordingly, DoD would not have an adequate baseline to effectively measure its Y2K progress. Additionally, DoD Components did not consistently interpret the DoD Chief Information Officer reporting requirements. The DoD Management Plan provides definitions for "system" and "mission-critical," but definitions were nonspecific and open to interpretation. Also, DoD did not establish clear reporting guidance and requirements. The report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), in the role of the DoD Chief Information Officer, update the DoD Management Plan to reflect changes in reporting requirements and include adequate procedures on how Y2K quarterly reports should reconcile. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred, stating that the DoD Management Plan would be updated accordingly.

Inspector General, DoD, Report No. 98-074, "Sharing Year 2000 Testing Information on DoD Information Technology Systems," February 12, 1998. The report states that DoD designated the use of homepages on the Internet as the primary means of sharing Y2K-related information, and DoD Components had made progress in establishing Y2K information on their respective homepages. However, the process for sharing Y2K testing information could have been more effective. The DoD Components could have been inefficiently spending time-sensitive resources in solving the Y2K problem through the duplication of efforts and in attempting to locate accurate testing information. The ability to retrieve and use all appropriate testing information in a timely and efficient manner would be instrumental in the solution of the Y2K problem.

The report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), as the DoD Chief Information Officer, establish a DoD-sponsored Y2K testing information center within DoD for gathering, analyzing, storing, and disseminating Y2K-related testing information and provide Y2K hotline services to the DoD Components. Further, the report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) formally notify the DoD Components that the Joint Interoperability Test Command is the DoD-sponsored Y2K testing information center responsible for fielding questions and providing information on Y2K testing and that DoD Components should provide various Y2K information to the Joint Interoperability Test Command. Finally, the report recommended that the Assistant Secretary of Defense (Command, Control,

Communications, and Intelligence) establish links on the Internet from high-level DoD homepages that allow DoD personnel searching for Y2K testing information to quickly and easily obtain the information gathered by the Joint Interoperability Test Command.

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with the recommendations of the report. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that his office had already directed the Joint Interoperability Test Command within the Defense Information Systems Agency to maintain a homepage that addresses Y2K testing information for all of DoD. The Draft DoD Management Plan states that the Defense Information Systems Agency was to designate the Joint Interoperability Test Command as the Y2K testing information clearinghouse for DoD. Further, the Joint Interoperability Test Command web site contains information on the following:

- Y2K testing guidelines,
- links to Y2K tools,
- Defense Information Systems Agency links and other related Y2K sites,
- test methods,
- vendor-provided data, and
- tool evaluations and lessons learned.

Additionally, the Draft DoD Management Plan states that DoD Components may use the Joint Interoperability Test Command for independent verification of systems, as required by the Office of Management and Budget.

Inspector General, DoD, Report No. 98-068, "Year 2000 Compliance in an Air Force Special Access Program," February 6, 1998. The report states that the Air Force Special Access Program Office did not complete a thorough computer systems inventory or perform a risk assessment. However, the program office took action on the deficiencies identified during the audit. The report recommended that the Air Force Special Access Program Office revise its program management plan to include an inventory and Y2K risk assessment of all computer systems; prepare a comprehensive test plan; and develop a plan to renovate, replace, or retire systems found to be noncompliant. Additionally, the report recommended that the Air Force Special Access Program Office revise the five-phase completion dates established in its program management plan to comply with the phase completion dates established by the Air Force. Management concurred with the findings and recommendations and agreed to take corrective actions.

Inspector General, DoD, Report No. 98-065, "DoD Information Technology Solicitations and Contract Compliance for Year 2000 Requirements," February 6, 1998. The report states that 20 of the reviewed 35 indefinite-delivery/indefinite-quantity and indefinite-delivery-requirement information technology contracts for commercial off-the-shelf products did not have the required Federal Acquisition Regulation Y2K compliance language, and none of

the 35 contracts required testing of purchased products. As a result, DoD had no assurance that information technology products offered or purchased were Y2K compliant. Further, the purchase of noncompliant products may have seriously hampered the ability of DoD to perform its administrative and warfighting mission requirements. Additionally, because 33 of the 35 contracts are available for use by other Federal agencies, nonconforming contract items could negatively affect the ability of the Federal Government to survive the Y2K crisis.

At the conclusion of the audit, the Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Director, Defense Procurement, began drafting new guidance for the DoD Components that would require Y2K-compliant information technology and testing of items purchased from the information technology contracts. The report made no recommendations because the actions taken addressed the findings of the report. The Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued the memorandum, " Acquisition of Year 2000 (Y2K) Compliant Information Technology (IT) and Bringing Existing IT Into Compliance," on December 18, 1997.

Army Audit Agency

Information Memorandum AA 98-350, "Medical Year 2000 Action Plans for Facilities and Infrastructure Systems," October 8, 1998. The memorandum states that the Raymond W. Bliss Army Health Center had begun to identify critical facility support systems that needed actions completed before becoming Y2K compliant. However, the vacancy of the Facilities Manager's position impacted the Army Health Center's effort to complete certification of its critical systems. As a result, the critical systems would not meet the mandated time frame designated by the Army Medical Command. Furthermore, the memorandum states that the following areas needed additional management emphasis: testing, documentation, Y2K implementation, setting priorities, and contingency planning. Because the review was conducted at multiple locations and the results would be included in an overall summary, the memorandum made no recommendations to the Army Health Center.

Memorandum, "Information for the Intelligence Annex of the Semiannual Report to Congress," October 5, 1998. The Army Audit Agency provided for inclusion into this report a memorandum to the Inspector General, DoD, that contains unclassified information for the Intelligence Annex of the Semiannual Report to Congress for the 6-month period that ended September 30, 1998. The Army Audit Agency issued three formal reports that involved intelligence-related Y2K oversight during the 6-month period that ended September 30, 1998. The memorandum provides a synopsis for the following reports that the Army Audit Agency issued titled " Year 2000 Compliance for Special Access Programs":

- Report No. AA 98-313
- Report No. AA 98-201
- Report No. AA 98-200

The audit covered the Y2K compliance efforts for Intelligence Special Access programs. The Army Audit Agency provided the following results. The product managers and personnel had generally established adequate efforts to prepare for Y2K. Generally, the program managers assigned responsibility, provided guidance, developed Y2K action plans, initiated compliance reviews, and instituted actions to modify contracts. One program manager needed to complete evaluations of a program's information systems and report the results, obtain certification and verification from external program managers, and complete contract modifications. However, a project leader needed to update the action plan to establish timelines. Additionally, a project leader and project coordinator needed to perform risk assessments, prepare contingency plans, develop cost estimates, and report results. The associated commands agreed to the following actions:

- establish reporting procedures;
- update the action plan;
- update hand receipts for information systems;
- identify and evaluate all instrumentation items for Y2K compliance;
- complete risk assessments, contingency plans, and cost estimates;
- obtain certification and verification from external program managers; and
- complete modifications for remaining contracts.

Information Memorandum AA 98-353, "Medical Year 2000 Action Plans for Facilities and Infrastructure Systems," September 24, 1998. The memorandum states that the Reynolds Army Community Hospital made sufficient progress in identifying the critical facility support systems to initiate actions needed for them to be Y2K compliant. However, facility managers did not expect to have the critical systems certified within the time frames mandated by the Army Medical Command. The memorandum identifies some areas that needed additional management emphasis related to reporting timely and accurate facility status reports, testing the systems and documenting the results, documenting coordination with outside entities, and developing specific Y2K contingency plans. The review indicated that facility equipment inventory lacked cost data and incorrectly reported compliance codes. The review also indicated that the Reynolds Army Community Hospital had not conducted compliance testing and it would not correct the conditions until March 1999. Additionally, the Reynolds Army Community Hospital had not submitted facility status reports to the Army Medical Command, and it did not develop Y2K contingency plans for untested systems. The memorandum suggested that the Reynolds Army Community Hospital do the following:

- submit timely and accurate facility status reports,
- test critical systems in accordance with the Army Medical Command guidance and document all testing performed,

- document contacts with outside entities, and

- develop specific Y2K contingency plans for noncompliant systems.

Memorandum Report No. AA 98-367, "Automated Information Systems-Year 2000 (Phase IV): Assessment of Selected Mission-Critical Systems at the Office of the Programs Executive Officer for Standard Army Management Information Systems," September 23, 1998. The memorandum states that the users of the Standard Installation and Division Personnel System were at high risk of potentially losing continuity-of-operations because of the Y2K. The mission-critical standard personnel system would not be fielded to all of its users before October 20, 1999. The memorandum indicates that the current fielding schedule, which already extends 10 months beyond the timeline established by the Army, is subject to possible slippage. Many users will not have ample time to test the standard personnel system within their environment and with unique interfacing systems. The memorandum suggested that the program manager of the standard personnel system do the following:

- establish and document definitive timelines for end-to-end testing between the standard personnel system and its interfacing systems no later than September 30, 1998, and

- identify trigger dates for disseminating contingency plans to all the users of the standard personnel system.

The program executive office representatives and the program manager fully agreed with the suggested actions.

Memorandum Report No. AA 98-366, " Automated Information Systems-Year 2000 (Phase IV): Assessment of the Arlington National Cemetery's Year 2000 Oversight Program," September 23, 1998. The memorandum states that the Y2K resolution progress for the Arlington National Cemetery Information Management System was rated as low risk. The Y2K non-information technology (infrastructure) assessments were rated as high risk. The memorandum indicates that responsible personnel did not provide reasonable assurance that actions were ongoing or plans were implemented. The Arlington National Cemetery managers and directors were not involved in assessing, managing, monitoring, or resolving Y2K vulnerabilities concerning the safety and security issues related to core mission requirements.

Additionally, responsible personnel did not report any non-information technology (infrastructure) items to the Army Y2K database. The memorandum suggested that the Arlington National Cemetery:

- identify all vulnerable Y2K infrastructure areas affecting safety and security issues and core mission requirements and determine how the missions would be impacted,

- report mission-critical systems and non-information technology (infrastructure) items to the Army Y2K database,

- identify and report all resource requirements to make non-information technology (infrastructure) areas Y2K compliant, and

- prepare Y2K contingency plans in the event that safety and security issues affect core mission requirements.

The Superintendent fully agreed with the suggested actions and initiated immediate actions to ensure continuity of cemetery operations.

Information Memorandum AA 98-351, "Medical Year 2000 Action Plans for Facilities and Infrastructure Systems," September 23, 1998. The memorandum states that the Patterson Army Health Clinic made progress in identifying and confirming that critical facility support systems were Y2K compliant within the time frames mandated by the Army Medical Command. However, some areas that needed additional management emphasis related to coordinating facility-wide Y2K efforts and oversight or validation of subordinate facilities at Fort Monmouth or at other installations. The review identified that oversight or validation of subordinate facilities at Fort Monmouth or other installations did not exist, and Patterson Army Health Clinic Information Management Division, Biomedical, and Facility groups needed better communication and coordination. The memorandum suggested that the Patterson Army Health Clinic:

- appoint a leader responsible for coordinating all Y2K compliance efforts and

- determine the Y2K status of subordinate facilities.

Information Memorandum AA 98-347, "Medical Year 2000 Action Plans for Facilities and Infrastructure Systems," September 23, 1998. The memorandum states that Winn Army Community Hospital made good progress in identifying and confirming that critical facility support systems were Y2K compliant within the time frames mandated by the Army Medical Command. However, two areas needed additional management emphasis relating to the identification of ancillary support systems and the development of specific Y2K contingency plans. The memorandum indicates that specific Y2K contingency plans needed to be developed, and personnel were concerned that the Army Medical Command systems may not meet the December 1998 deadline.

Memorandum Report No. AA 98-332, "Automated Information Systems-Year 2000 (Phase IV): Assessment of Selected Mission-Critical Systems at the Office of the Chief Army Reserve," September 23, 1998. The memorandum states that the functional proponents throughout the Office of the Chief, Army Reserve, needed to become more actively involved in managing, monitoring, and resolving Y2K issues that could cause loss to core mission capability within their business areas of responsibility. The Y2K strategy for the Army Reserve requires successful fielding of the Reserve Component Automated System. If the infrastructure that supports the Reserve Component Automated System was not fielded in time, it could adversely affect continuity of operations throughout the Army Reserve. Additionally, two mission-critical systems maintained by the Office of the Chief, Army Reserve, were at high risk of failing on or before Y2K.

The audit concluded that the Army Reserve was at high risk of potentially losing continuity of operations and its capability to conduct core mission requirements because of the Y2K. The memorandum suggested that the Chief, Army Reserve, take the following actions:

- make Y2K a top command priority throughout the Army Reserve;

- identify mission-critical systems core to the mission of the Army Reserve and assess how Y2K would affect operations;

- identify and report all resource requirements to make mission-critical systems Y2K compliant;

- prepare test plans that address interfacing systems, timelines, and who and where Y2K testing would be performed in coordination with functional business area managers;

- identify and report all mission-critical internal and external interfaces and assess the impact on resource needs to make them Y2K compliant; and

- prepare contingency plans in accordance with the Army Action Plan.

The Chief Information Officer fully agreed with the suggested actions.

Report No. 98-363, "U.S. Army Europe, and Seventh Army's Progress Towards Year 2000 Compliance," September 22, 1998. The review was conducted from February to July 1998. The report states that the U.S. Army Europe and Seventh Army made adequate progress toward Y2K compliance. However, U.S. Army Europe and Seventh Army needed to continue to monitor progress because many of the unique systems were at moderate risk of noncompliance. The report indicates that some unique systems had the following moderate risks:

- technical risk because of the complexity of the Y2K solution strategy for the system and the dependency on external interfaces with standard systems,

- time risk because of the lack of adequate time needed to fix and test an application and related interfaces, and

- resource risk because of the shortfalls in available funding to fix the system.

The report suggested that the U.S. Army Europe and Seventh Army take the following actions:

- monitor the progress of systems with moderate compliance risk to ensure appropriate action;

- instruct program managers to identify Y2K compliance status of interfacing systems;

- instruct program managers to prepare interface agreements;

- instruct program managers to prepare contingency plans, with identified trigger dates, in the event of slippage of compliance strategy timelines or late fielding or failure of compliant interfaces;

- instruct local program managers to coordinate with standard system program managers to identify Y2K issues with their related systems; and

- instruct local functional proponents to assess the operational impact and possible loss of functionality if standard systems fail or are fielded late. The U.S. Army Europe and Seventh Army was to closely monitor the status of the fielding dates and prepare contingency plans if the fielding date slipped.

Memorandum Report No. AA 98-335, "Morale, Welfare and Recreation Year 2000 Management Information Systems," September 22, 1998. The review was conducted from July through August 1998. The memorandum states that the Army Recreation Machine Program made adequate progress toward Y2K compliance of its automated systems. However, it needed to continue to monitor progress because three of its five unique systems were at moderate risk of noncompliance. The memorandum indicates that some unique systems had moderate technical risk, because of the complexity of the Y2K solution strategy for the system and because of the lack of contingency plans and interface agreements, and time risk because of the lack of adequate time needed to fix and test an application and related interfaces. The memorandum suggested that the Army Recreation Machine Program:

- monitor the progress of systems with moderate compliance risk to ensure that appropriate action was taken; and

- instruct program managers to prepare and document contingency plans with identified trigger dates in the event of slippage of compliance strategy timelines.

Information Memorandum AA 98-342, "Medical Year 2000 Action Plans for Facilities and Infrastructure Systems," September 21, 1998. The memorandum states that Darnall Army Community Hospital made adequate progress in identifying and confirming that critical facility support systems were Y2K compliant. Facility managers expected to have the critical systems certified within the time frames mandated by the Army Medical Command. However, some areas needed additional management emphasis relating to testing the systems and documenting the results, developing specific Y2K contingency plans, and improving coordination and communications among the separate facility Y2K compliance efforts. The review indicates that the Darnall Army Community Hospital did not perform or schedule testing and did not develop Y2K-specific contingency plans.

Information Memorandum AA 98-348, "Medical Year 2000 Action Plans for Facilities and Infrastructure Systems," September 18, 1998. The memorandum states that the William Beaumont Army Medical Center made sufficient progress in identifying the critical facility support systems and initiating actions needed for them to be Y2K compliant. Facility managers expected to have the critical systems certified within the time frames mandated by the Army Medical Command. However, some areas needed additional management emphasis relating to testing the systems and documenting the results, submitting

facility status reports, developing specific Y2K contingency plans, and monitoring related actions ongoing at subordinate medical activities. The William Beaumont Army Medical Center did not fully document testing or schedule testing for all systems. The William Beaumont Army Medical Center also did not submit facility status reports to the Army Medical Command or develop specific Y2K contingency plans. Additionally, the William Beaumont Army Medical Center Information Management Division, Biomedical, and Facility groups needed better communication and coordination. The memorandum suggested that the William Beaumont Army Medical Center do the following:

- test critical systems in accordance with the Army Medical Command guidance,
- document all testing performed,
- submit timely and accurate facility status reports,
- develop specific Y2K contingency plans,
- appoint an individual to coordinate all Y2K efforts,
- provide oversight and guidance to subordinate activities on Y2K matters, and
- request and validate Y2K activity facility status reports.

Memorandum Report No. AA 98-344, "Medical Year 2000 Action Plans for Facilities and Infrastructure Systems (M8121C)," September 18, 1998. The memorandum states that the Tripler Army Medical Center adequately identified and assessed facility support systems for Y2K compliance. However, one critical system would not be completed within the time frame mandated by the Army Medical Command. The Tripler Army Medical Center funded a project to replace the system by July 1999. Although no specific Y2K contingency plan existed, the facility's engineers would follow the Medical Center's Emergency Preparedness Plan if critical systems failed in Y2K. The memorandum suggested that the Medical Command waive its December 1, 1998, Y2K compliance deadline for the heating, ventilation, and air conditioning control system based on funded system replacement that would achieve compliance by July 30, 1999.

Also, the memorandum states that the Tripler Army Medical Center needed clearer guidance from the Army Medical Command on necessary Y2K testing of biomedical systems. The Army Medical Command shifted its testing policy from minimal to extensive because the manufacturer's claims that systems were compliant were proven false. The extensive testing was considered expensive, and some critical systems could fail during testing and endanger the patients of the Tripler Army Medical Center. The memorandum concludes that the Tripler Army Medical Center could not accomplish the necessary testing unless the Army Medical Command facilitated the efforts of the Tripler Army Medical Center or extended the deadline for testing biomedical systems beyond December 1, 1998.

Report No. AA 98-355, "Morale, Welfare and Recreation Year 2000 Management Information Systems (Assignment Code M8-119C), September 17, 1998. The report states that, overall, the U.S. Army Forces Command provided good guidance and oversight for managing the Y2K compliance of the Fort Campbell morale, welfare, and recreation activities. Fort Campbell did not obtain all vendor certifications or test key hardware. Additionally, Fort Campbell did not develop contingency plans to ensure that morale, welfare, and recreation businesses could continue in spite of Y2K failures. The memorandum suggested that the U.S. Army Forces Command direct all subordinate commands to:

- perform real-time testing of systems determined to be Y2K compliant;

- prepare contingency plans for systems not tested or that fail to ensure the continuance of morale, welfare, and recreation business activities; and

- require vendors to certify Y2K compliance of all off-the-shelf systems and include requirements for Y2K compliance in all system contracts.

Information Memorandum AA 98-354, "Morale, Welfare and Recreation Year 2000 Management Information Systems (Assignment Code M8-119C), September 17, 1998. The memorandum states that the Army Materiel Command provided excellent guidance and oversight for managing Y2K compliance at Redstone Arsenal and Aberdeen Proving Ground morale, welfare, and recreation activities. Specifically, the memorandum states that the Y2K action plan of the Army Materiel Command provides an excellent framework for ensuring that systems would be Y2K compliant and that adequate funds would be available to complete the necessary renovations and replacements. However, the subordinate commands needed to develop contingency plans and prepare to execute the plans if systems failed.

The memorandum states that the test plans of the Army Materiel Command contained excellent guidance for subordinate commands. The test plans of the Army Materiel Command were part of its action plan. The test strategy called for testing at several levels, including unit, integration, and systems testing on software, hardware, and firmware. The strategy included test planning, preparation, execution, documentation, evaluation, and tools. Additionally, the Army Materiel Command required its subordinate commands to develop new contingency plans or revise current backup and recovery plans to reflect any changes made because of Y2K compliance. Finally, the memorandum states that the Army Materiel Command and its subordinate commands made adequate progress identifying major business systems and committing appropriate resources to make Y2K corrections.

The memorandum suggested that the Army Materiel Command direct all subordinate commands to perform real-time testing based on Y2K dates when fielded systems were determined to be Y2K compliant and to test vendor-certified fielded systems. The memorandum also suggested that, for those systems that fail or that cannot be tested, the Army Materiel Command require subordinate commands to have the appropriate office develop contingency plans to ensure continuance of morale, welfare, and recreation businesses in case of possible Y2K failures.

Information Memorandum AA 98-349, "Medical Year 2000 Action Plans for Facilities and Infrastructure Systems," September 17, 1998. The memorandum states that the Eisenhower Army Medical Center made very good progress in identifying and confirming that critical facility support systems were Y2K compliant within the time frames that the Army Medical Command mandated. However, the memorandum suggested that the Eisenhower Army Medical Center take the following actions:

- develop protocols and conduct system tests for critical Y2K dates when testing could be accomplished safely, effectively, and efficiently;

- develop system-specific Y2K contingency plans when manufacturer assurance is not available and testing is not practical; and

- provide guidance to subordinate facilities for developing testing and Y2K contingency plans.

Information Memorandum AA 98-352, "Medical Year 2000 Action Plans for Facilities and Infrastructure Systems," September 15, 1998. The memorandum states that the Fox Army Health Center made adequate progress in identifying and confirming that critical facility support systems would be Y2K compliant; however, facility personnel believed that certification would not be achievable by December 1998. The memorandum states that personnel were confident that contracts would be in place by September 30, 1998, and that certification would be completed by September 30, 1999. The memorandum identifies areas that needed additional management emphasis related to the inventory and assessment of building infrastructure items, developing a specific Y2K contingency plan, and obtaining a specific Y2K compliance assurance from manufacturers. The memorandum suggested that the Fox Army Health Center do the following:

- perform another inventory and assessment of facility items,

- report all items that had Y2K implications in the monthly Y2K status report,

- develop and obtain approval for a Y2K contingency plan, and

- obtain letters of assurance from manufacturers for those items that were identified as Y2K compliant.

Information Memorandum AA 98-345, "Medical Command's Year 2000 Action Plans for Facilities and Infrastructure Systems," September 15, 1998. The memorandum states that the Madigan Army Medical Center (the Center) made excellent progress in identifying and assessing that critical facility support systems would be Y2K compliant within the time frames mandated by the Army Medical Command. The Center was to test critical systems and conduct a training session on testing at the request of the Army Medical Command for other medical treatment facilities. The report suggested that the Center prepare Y2K contingency plans.

Information Memorandum AA 98-346, "Medical Year 2000 Action Plans for Facilities and Infrastructure Systems," September 11, 1998. The memorandum states that the Evans Army Community Hospital made good progress in identifying and assessing critical facility support systems for Y2K compliance and committed funds for replacement systems. However, facility managers did not expect to meet the Army Medical Command requirements for certification by December 1998. The memorandum states that the Evans Army Community Hospital did not conduct testing and had no oversight or validation of subordinate facilities. Further, the Evans Army Community Hospital was in danger of not completing its projects to replace noncompliant systems by Y2K. The memorandum suggested that the Evans Army Community Hospital do the following:

- appoint a lead person to be responsible for coordinating all Y2K compliance efforts,
- develop Y2K-specific contingency plans, and
- determine the Y2K status of subordinate facilities.

Information Memorandum AA 98-343, "Medical Year 2000 Action Plans for Facilities and Infrastructure Systems," September 9, 1998. The memorandum states that the Brooke Army Medical Center made good progress in identifying and confirming that critical facility support systems were Y2K compliant within the time frames mandated by the Army Medical Command. However, some areas needed additional management emphasis on submitting facility status reports, developing specific Y2K contingency plans, and providing detailed guidance to subordinate medical activities. The memorandum indicates that the Brooke Army Medical Center did not provide facility status reports to the Army Medical Command or prepare specific Y2K contingency plans. Additionally, the Brooke Army Medical Center Information Management Division, Biomedical, and Facility groups needed better communication and coordination. The memorandum suggested that the Brooke Army Medical Center take the following actions:

- submit timely and accurate facility status reports to the Army Medical Command,
- develop specific Y2K facility action plans,
- develop and issue guidance to subordinate facilities, and
- appoint a Y2K lead responsible for coordinating all Y2K efforts.

Report No. AA 98-331, "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: Combat Service Support Control System (CSSCS)," September 3, 1998. The report states that the Y2K assessment of the Combat Service Support Control System identified it as low risk for Y2K failure. Although the product manager had been aggressive in addressing key Y2K issues, two issues required management involvement. One issue was the interface agreement between the interface partner that manages the Maneuver Control System; the Program

Manager for the Maneuver Control System had not provided any response to the Combat Service Support Control System project manager on the interface issues. A second issue was that the Combat Service Support Control System Project Manager completed the Army Y2K certification compliance checklist; however, the Project Manager had not received acknowledgment from the Program Executive Office representatives about the approval status. As a result of the assessment, the Program Executive Office stated that it agreed with the issues identified and planned to review, approve, and forward the checklist as required. Also, the Program Executive Office responded that memorandums of agreement with an outside service or agency were to be signed by the highest-ranking official with control and responsibility for the outside interface.

Memorandum Report No. AA 98-327, "Morale, Welfare and Recreation Year 2000 Management Information Systems (H8112J), September 2, 1998. The memorandum states that the information and non-information technology action plans for the Eighth U.S. Army provided the morale, welfare, and recreation organizations with adequate guidance to ensure that needed resources were identified and that required systems would be Y2K compliant. However, the Morale, Welfare, and Recreation Division needed to complete its draft action plan and needed to expedite its progress in identifying major systems and quantifying the resources needed to make cost-effective Y2K corrections. The memorandum suggested that the Eighth U.S. Army ensure that:

- the Morale, Welfare, and Recreation Division and support activities expedite the assessment phase of their action plans;

- the Management Information Systems Branch complete the matrix needed to assess and report systems for the information and non-information technology action plans; and

- the support groups and the Morale, Welfare, and Recreation Division identify information and non-information technology systems that are essential to the morale, welfare, and recreation core mission and estimate the resources needed to make the revisions necessary for Y2K compliance.

Memorandum Report No. AA 98-328, "Morale, Welfare and Recreation Year 2000 Management Information Systems (H8112K), September 1, 1998. The report assesses progress toward resolving Y2K issues for morale, welfare, and recreation programs at Army installations within U.S. Army Pacific. The report states that the U.S. Army Pacific did not have a specific action plan for making morale, welfare, and recreation systems Y2K compliant. The U.S. Army Garrison Hawaii had an informal program to ensure Y2K compliance of all management information systems, but the program did not include non-information technology systems.

The Garrison's Directorate of Community Activities inventoried management information systems and identified 164 morale, welfare, and recreation management systems from nonappropriated fund activities that were not Y2K compliant. The report states that the systems identified were expected to be compliant by October 1, 1999, provided that the Directorate's management information systems team of three could make all the necessary patches and install new computers. In addition, the team also needed to support 204 systems for the Directorate's appropriated fund activities, evaluate patches and replacement of

non-information technology systems, and conduct normal information systems activities. The report states that the team may have needed additional personnel to assist them.

The Office of the Deputy Chief of Staff for Personnel, U.S. Army Pacific, and the Garrison's Directorate of Community Activities were focused on management information technology systems and overlooked non-information technology systems for which they might be responsible. The Deputy Chief of Staff for Personnel, U.S. Army Pacific, and the Garrison's Directorate of Community Activities assumed that the Deputy Chief of Staff for Engineering and the Garrison's Directorate of Public Works were responsible for non-information technology systems.

The report suggested that the U.S. Army Pacific issue guidance to its installations with instructions to accomplish the following:

- identify and inventory all nonappropriated fund systems essential to morale, welfare, and recreation activities and assess the systems to determine the necessary compliance corrections;

- test compliance to ensure that systems would operate in the Y2K;

- determine resource requirements to make the systems compliant and, if sufficient resources were not available, prioritize systems for compliance revisions based on the mission impact; and

- develop contingency plans for operations for those systems that would not be fixed by Y2K.

Additionally, the report suggested that the U.S. Army Pacific direct installation Directorates of Community Activities to coordinate with Directorates of Public Works concerning non-information technology systems so that both organizations were aware of the systems that they needed to make Y2K compliant.

Report No. AA 98-326, "Morale, Welfare and Recreation Year 2000 Management Information Systems (Assignment Code M8-119C), August 26, 1998. The report assesses plans and actions to resolve Y2K issues for morale, welfare, and recreation management information systems at the Army Training and Doctrine Command, Fort Monroe, Virginia, and the Army Armor Center and Fort Knox, Kentucky. The report states that the Y2K action plan of the Training and Doctrine Command provided a framework for ensuring that systems would be Y2K compliant and that adequate funds would be available to complete necessary renovations and replacements. However, Fort Knox needed to develop contingency plans and be prepared to execute the plans if the systems failed.

Fort Knox inventoried all of its business systems, developed a list of systems to be replaced, and budgeted for replacement of the systems. The report states the following of the managers at Fort Knox:

- they were aware of the Y2K problem,

- they did real-time tests of equipment to determine compliance, and

- they had contingency plans for dealing with power and cash register failures because of frequent power outages on post.

The report suggested that the Training and Doctrine Command direct all subordinate commands to perform real-time testing based on Y2K dates when fielding systems determined to be Y2K compliant. Additionally, the report suggested that the subordinate commands develop contingency plans for systems that were not tested.

Report No. AA 98-322, "Automated Information Systems-Year 2000 (Phase IV); Assessment of Selected Mission-Critical Systems at the U.S. Army Reserve Personnel Command," August 25, 1998. The report states that the Y2K management oversight program established by the Army Reserve Personnel Command senior leadership was ineffective in monitoring, tracking, and resolving Y2K issues. As a result, the command was at risk of potentially losing continuity-of-operations and its capability to conduct core requirements. The responsible command personnel had not accomplished the following:

- included functional directorates with the identifying risks and operational impacts,

- addressed all the critical and pertinent information essential for preparing effective system interface agreements,

- coordinated contingency plans with functional directorates to ensure that user-related issues were identified and addressed,

- identified or committed resources or both to ensure achievement of Y2K compliance, and

- provided reasonable assurance that some of the critical systems were on target with meeting the established DoD and Department of the Army milestones.

The suggested actions included requiring functional directorates to:

- identify mission-critical systems core to their business areas and how Y2K would affect their operations,

- report system inventories to the Y2K database,

- identify and report all resource requirements to make their mission-critical systems Y2K compliant,

- identify and report all mission-critical internal and external interfaces and assess the impact on resource needs to make critical systems Y2K compliant, and

- coordinate and reevaluate contingency plans to address roles and responsibilities for key personnel and trigger dates for implementing contingency plans.

The Commander, Army Reserve Personnel Command, agreed with the assessment and directed the responsible command personnel to establish a Y2K Project Office to resolve all issues identified.

Report No. AA 98-321, "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: All Source Analysis System (ASAS)," August 25, 1998. The report states that the users of the All Source Analysis System were at moderate risk of potentially losing continuity of operations by the Y2K. Moderate risk requires close monitoring of ongoing or planned actions, recognizes that resources are available but may not be readily sufficient to complete the remediation work effort, and recognizes that users could recover from slippages but might not have enough time to complete and verify any changes made. As a result, the lack of interface identification was a potential risk. The project personnel agreed, stating that the agreements had not been developed because of a lack of dialogue between Army personnel and personnel from non-Army organizations. Therefore, the suggested actions cited required that the project manager coordinate the agreement effort with the interface partners and update the Army Y2K database to accurately reflect all the systems that interface with the All Source Analysis System. Management agreed with the suggested actions and began to resolve the issues.

Report No. AA 98-311, "Automated Information Systems-Year 2000 (Phase IV); Assessment of Selected Army Air Traffic Control Mission-Critical Systems," August 13, 1998. The review was conducted from July 7 through July 16, 1998. The report addresses the Y2K assessment of two mission-critical air traffic control systems. The report states that the Army Aviation and Missile Command did not adequately manage or address Y2K remediation efforts, and contractors were still assessing the Y2K impact to both systems. As a result, the personnel could not prepare risk management plans, test plans, contingency plans, or system interface agreements. Also, the mission-critical database was incorrect because nine mission-critical systems had been omitted. Additionally, oversight for compliance and identification of operational risks associated with system interfaces was lax. The report suggested that the Army Aviation and Missile Command initiate actions directing the contractors to complete and provide detailed Y2K mission-critical system assessments. Also, the Army was to establish effective oversight of the systems by reporting them in the Y2K database and report those systems that are behind scheduled timelines. Further, the Army was to establish and implement procedures to highlight how the management of non-Army-maintained air traffic control solutions could adversely impact Army mission requirements and operations. The Army was to establish procedures that required operational assessments and contingency plans to be prepared in case systems failed to be fixed or fielded within an acceptable time frame. The Command agreed with the suggested actions.

Report No. AA 98-310, "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," August 13, 1998. The report discusses Y2K progress for the Army system entitled Transportation Coordinators-Automated Information for Movement System II. Although the system was designated as mission critical, the report states that because the system was not directly impacted by a Y2K timeline, it would replace multiple cross-service legacy systems. As a result, the system currently being fielded was to be Y2K compliant. The report recommended that the Program Executive Office Standard Army Management Information Systems identify all mission-critical interfacing systems and prepare interface memorandums of agreement for each system interface. Also, the Program Executive Office was to update the Y2K database documenting the interfaces as well as update and revise the testing plan to ensure that interfaces were properly tested for Y2K flaws. The Program Executive Office Standard Army Management Information Systems agreed with the recommendations.

Report No. AA 98-309, "Automated Information Systems-Year 2000 (Phase IV); Assessment of Selected Mission-Critical Systems at the U.S. Army Reserve Command," August 13, 1998. The review was conducted during June 1998. The report states that the Army Reserve Command Y2K strategy had not been adequately implemented. Functional proponents were not actively involved in managing, monitoring, and resolving Y2K issues. The Command needed more involvement to ensure that Y2K would not adversely affect the continuity of operations and cause them to lose the capability to conduct core mission requirements. Recommendations of specific actions included the following:

- identifying mission-critical core systems to their business areas and how the Y2K would affect operations;

- reporting system inventories in the Y2K database;

- identifying and reporting all resource requirements needed for Y2K compliance; and

- identifying, reporting, and assessing internal and external interfaces.

The Command fully agreed with the recommendations and directed the establishment of a milestone plan to resolve all issues.

Memorandum Report No. AA 98-291, "U.S. Southern Command Year 2000 Issues," July 31, 1998. The review was conducted during April 1998. The report states that U.S. Southern Command personnel needed to continue to identify and address "high risk" issues. Also, the U.S. Southern Command needed to ensure that all mission-critical systems operate adequately and that Joint, DoD, Service, and agency personnel provide timely and pertinent information related to fixing, testing, certifying, and fielding mission-critical systems affected by Y2K. As a result, the report made recommendations to the Commander in Chief, U.S. Southern Command, and the Director, Joint Staff.

The actions directed to the Commander in Chief were as follows:

- require the U.S. Southern Command Component Commanders to update the Headquarters, U.S. Southern Command, quarterly on the Y2K compliance progress;

- require the U.S. Southern Command Directors to update U.S. Southern Command personnel quarterly on the status of the Y2K oversight program;

- establish a process to identify and resolve Y2K assessment issues of adverse impacts on theater mission capabilities, including the systems that Joint, DoD, Service, and agency program offices provided;

- ensure that U.S. Southern Command Directors perform operational impact assessments of functional business areas and prepare contingency plans for the continuity-of-mission operations and requirements; and

- identify interface systems, including allied and coalition systems, and develop system interface agreements or an equivalent mutual agreement of understanding.

Actions directed to the Director, Joint Staff, required personnel to work with Services and agencies to identify systems not meeting Y2K target timelines.

The U.S. Southern Command provided comments on September 8, 1998, stating that actions had been taken to get the U.S. Southern Command components more involved in assessing Y2K issues. The U.S. Southern Command concurred with the recommendations and stated that it is actively tracking progress through status update requests and action-officer-level interface. Also, it is posting documents and briefs on its webpage, and it is actively engaged in the identification and resolution of DoD-wide system issues. The U.S. Southern Command expected the centralized database discussed at the Y2K Warfighters Conference in August 1998 to be a valuable tool in assisting the effort. The Y2K officer had established trigger dates for contingency plans to be established based on Y2K-compliant status and dates of individual system implementation. The U.S. Southern Command was to update its quarterly report submission to the Joint Staff to indicate when interfaces were identified and interface agreements implemented. The Joint Staff did not respond to the recommendations.

Memorandum Report No. AA 98-292, "U.S. European Command Year 2000 Issues," July 30, 1998. The review was conducted from February through March 1998. The report states that U.S. European Command personnel were not able to deal with unexpected system failures and fielding delays of Joint and DoD mission-critical standard systems that were affected by Y2K issues and used by the command to perform core mission requirements. Joint, DoD, Service, and agency system program managers responsible for fixing the standard systems were to provide U.S. European Command personnel with information related to fixing and fielding the systems so that Command personnel could effectively plan for contingencies. Management concurred with the findings and initiated actions to resolve the issues. The report made recommendations to the Commander in Chief, U.S. European Command, and the Director, Joint Staff.

The actions directed to the Commander in Chief, U.S. European Command, were as follows:

- require the U.S. European Command Component Commanders to update the Headquarters, U.S. European Command, quarterly on their Y2K compliance progress;

- require the U.S. European Command Directors to update U.S. European Command personnel quarterly on the status of the Y2K oversight programs;

- establish a process to identify and resolve Y2K assessment issues of adverse impacts on theater mission capabilities, including the systems provided by Joint, DoD, Service, and agency program offices;

- ensure that U.S. European Command Directors perform operational impact assessments of functional business areas and prepare contingency plans for the continuity-of-mission operations and requirements; and

- identify interface systems, including allied and coalition systems, and develop system interface agreements or an equivalent mutual agreement of understanding.

Actions directed to the Director, Joint Staff, required the following:

- personnel to work with Services and agencies to identify systems not meeting Y2K target timelines and

- the Joint Staff to ensure that Headquarters, U.S. European Command, and the supported unified command capture the Y2K issues of the U.S. Special Operations Command Europe.

In August 1998, the U.S. European Command concurred with all recommendations and tasked components to report monthly on 10 functional areas' Y2K compliance status. The Headquarters, U.S. European Command, Y2K Plan signed in May 1998 increases Director involvement and requires quarterly status reports of system listings and priorities. Although the command concurred with the recommendation to establish a process to identify and resolve Y2K issues, the task required assistance from Joint Staff, Service, and agency program managers. As a result, a centralized database accessible to functional users was offered as a solution, and the Director, Joint Staff, committed to resolve the issue. Command personnel would perform operational evaluations while performing system-level testing in the functional areas. In addition, the command personnel partially concurred with the recommendation to identify interface systems, including allied and coalition systems, and develop systems interface agreements. The inclusion of all allied and coalition systems was dependent upon efforts by the Joint Staff and the State Department. Comments were not received from the Joint Staff.

Report No. AA 98-213, "U.S. Army Audit Agency Assessment of U.S. Naval Forces Europe's Year 2000 Program," June 30, 1998. The review was conducted in February 1998. The report states that the U.S. Naval Forces Europe had no reasonable assurance that all mission-critical systems would be Y2K compliant. The report identifies the following issues for improvement: Y2K

management, risk assessment, and operational impact. The assessment found no action plan for Y2K, and the Y2K management effort consisted of two people working on the Y2K issue as an additional duty. Also, U.S. Naval Forces Europe did not identify Y2K points of contacts within the directorates, staff sections, or subordinate commands. Furthermore, the U.S. Naval Forces Europe did not assess how Y2K failure would impact operations, and assessments had not been performed to identify and document mission-critical systems, Y2K issues and solutions, and system interface agreements. Overall, the U.S. Naval Forces Europe had no requirement to update its Y2K progress to monitor the operational impact that could result from Y2K disruptions. The report provided the following suggested actions to the U.S. Naval Forces Europe:

- finalize the overall Y2K Action Plan for the Deputy Commander to sign and endorse to prioritize issues;

- strengthen the emphasis to develop, document, and distribute contingency plans and risk assessments, interface agreements, and test plans in accordance with Navy Y2K guidance; and

- establish a process to identify and report standard and joint high-risk systems with the potential for failure and disruption in Y2K.

"Automated Information Systems Year 2000 Department of the Army (DA) Functional Proponent Year 2000 Oversight Programs," May 20, 1998. The Army Audit Agency issued the following reports with that title:

Report No. AA 98-221, Memorandum for Deputy Chief of Staff for Operations and Plans

Report No. AA 98-220, Memorandum for Program Analysis and Evaluation Directorate

Report No. AA 98-219, Memorandum for Deputy Chief of Staff for Intelligence

Report No. AA 98-218, Memorandum for Deputy Chief of Staff for Personnel

Report No. AA 98-217, Memorandum for Deputy Chief of Staff for Logistics

Report No. AA 98-216, Memorandum for Assistant Chief of Staff for Installation Management

Report No. AA 98-215, Memorandum for Assistant Secretary of the Army (Financial Management and Comptroller)

Report No. AA 98-214, Memorandum for Assistant Secretary of the Army (Manpower and Reserve Affairs)

Report No. AA 98-212, Memorandum for Assistant Secretary of the Army (Research, Development, and Acquisition)

The reports discuss the initial and follow-on assessments of the Army Y2K oversight program. As a result of the follow-on assessment, the functional proponents had improved their Y2K oversight programs since the initial assessment. However, the report recommended that the Army take immediate action to accomplish the following:

- establish visibility to ensure that mission-critical systems identified in the operations and the planning business areas would be fixed,

- identify available resources for repairing Y2K solutions,

- conduct Army-wide risk management planning (to include at the system owner level) for the business area assessments and monitor all planning efforts,

- conduct Army-wide contingency planning,

- ensure development of system interface agreements, and

- review and sign Y2K certification compliance checklists.

In addition, the report recommended that the functional proponent take the following actions:

- designate the personnel and resources necessary to develop and execute the Y2K oversight program for the functional area assigned,

- form a working group made up of key functional area representatives to oversee the systems and devices that the key representatives manage,

- develop a plan to include input from major players and to contain key elements essential for managing Y2K, and

- work directly with Y2K points of contact to assess how other Y2K programs would affect the continuity of operations within the organization's functional business area.

Ongoing actions by the Army Chief Information Officer included conducting routine assessments of Y2K solutions and designating Y2K as a command interest item. Also, the Army clearly assigned the responsibility for fixing the problem, and schedules were executable. Further, testing and certification of the solutions were planned, and contingency plans existed for systems at risk. The information in the Y2K database was being reviewed for completeness and accuracy. In addition, the Director of Information Systems for Command, Control, Communications, and Computers was to review the quarterly reports personally, and recommendations were to be provided directly to the personnel responsible for the systems.

Report No. AA 98-197, "The Office of the Program Executive Officer for Command, Control, and Communications Systems," April 21, 1998. The report identifies that the Army needed greater emphasis to ensure that mission-critical systems would be compliant by the target date and that accurate information would be reported in the Y2K database. Additionally, Y2K duties

and responsibilities needed to be formalized and included in the performance standards of responsible officials. The command agreed with the findings and the suggested actions as follows:

- document and include Y2K duties in the performance standard and

- provide written instructions outlining the duties and responsibilities for managing the Y2K crisis and, as a minimum, provide the status of progress with all required Y2K data; develop, document, and distribute contingency plans; and report systems without contingency plans in the assessment phase.

Report No. AA 98-194, "Corps of Engineers Financial Management System-Year 2000," April 16, 1998. The report states that the Corps of Engineers needed to improve oversight of its Y2K program, accuracy and completeness of the Y2K database, and testing of Y2K solutions. Specifically, the Corps of Engineers did not develop and document the Y2K program strategy to include completion schedules, risk assessments, and contingency and testing plans. Also, the Corps of Engineers did not appoint a program manager to resolve problems and set Y2K priorities. The Corps of Engineers needed to ensure that database submissions include phase completion, estimated completion date, termination date with replacement system name, and the effective date. Furthermore, testing had not been developed agency-wide, limiting the chances that testing would occur between all interfacing systems. As a result, the report made the following recommendations to the Corps of Engineers:

- prepare a formal consolidated program strategy to document completion schedules, risk assessments, and testing and contingency plans;

- appoint a program manager to manage the Y2K program;

- provide quarterly updates to the Army Y2K database;

- validate the completeness and accuracy of the Army Y2K database submissions;

- prepare Corps-wide and system-specific testing plans; and

- request the Corps Internal Review Office to perform audit followup to determine whether Y2K compliance would be achieved by the mandated time frames.

Report No. AA 98-227, "Automated Information Systems Year 2000, U.S. Army National Guard," April 7, 1998. The report states that potential risk areas required immediate attention. Specific concerns were related to limited resources for Y2K revisions, testing of commercial off-the-shelf software, and developing contingency plans. Also, responsible personnel did not develop and document key strategic plans to address critical areas essential to mission-critical systems becoming Y2K compliant. The strategic planning documents (risk management plans, contingency plans, and test plans) were either missing or personnel did not adequately prepare the strategic planning documents. Also, personnel did not prepare and sign all system interface agreements. The Army Audit Agency directed recommendations to the Chief, National Guard Bureau, and the Director, Army National Guard.

Recommendations to the Chief, National Guard Bureau, were as follows:

- ensure that the program manager for the Reserve Automation System provide monthly updates to the Army National Guard Directorate on the Y2K compliance status and interface agreements and

- direct the program manager for the Reserve Component Automation System to develop risk management and contingency plans.

Recommendations to the Director, Army National Guard, were as follows:

- ensure that functional proponents have elevated Y2K system solutions of their mission-critical systems to priority one,

- require that functional proponents report the status of their Y2K system solutions quarterly to the Army Information Systems Branch,

- direct the timely completion of system interface agreements between all Guard systems and their respective interfaces,

- develop comprehensive risk management plans in accordance with the Army revised Y2K Action Plan - Revision II (dated April 1998) and address risks before they negatively impact mission-critical systems' abilities to reach or demonstrate Y2K compliance,

- develop comprehensive contingency plans in accordance with the Army revised Y2K Action Plan - Revision II (dated April 1998) based on the associated risks identified in the risk management plans, and

- establish "trigger dates" for implementation of the contingency plans to ensure sufficient time to achieve Y2K compliance.

Report No. AA 98-167, "Automated Information Systems Year 2000, Standard Installation and Division Personnel System 3," March 31, 1998. The report discusses Y2K issues that needed immediate attention. A review of the testing, fielding, and risk management plans showed that the testing and risk management plans did not address key issues that could have a material effect on the Standard Installation and Division Personnel System 3. Also, the report states that contingency plans were not coordinated or developed with the system users, the interfacing system owners, or the Department of the Army functional proponent. As a result, the report made suggested actions to the Program Executive Office and the Program Manager for the Standard Installation and Division Personnel System 3.

The report recommended that the Program Executive Office accomplish the following:

- review all data elements in the database for completeness and accuracy, and if changes are required, ensure that the system program manager is aware of the changes and

- require the Program Manager for the Standard Installation and Division Personnel System 3 to address potential risk areas identified during the Y2K assessment.

The report recommended that the Program Manager for the Standard Installation and Division Personnel System 3 accomplish the following:

- review the information in the database to ensure completeness and accuracy, and update the information as needed for the quarterly data calls;

- revise the risk management plan to include risks from all viewpoints (customer, user, activity, and functional proponent) and risks associated with fielding, funding, manpower, slippage, interfaces, testing, functionality, and the Reserve component;

- establish definitive time frames and Y2K test criteria for the Standard Installation and Division Personnel System 3 and increase the management and oversight for the testing and certification for all system interfaces and components;

- regularly monitor the fielding plan to guard against slippage and provide end users with the fielding schedule;

- identify areas in the fielding plan for which time could be condensed or accelerated to reduce the current planned fielding of the remaining sites;

- ensure that the required signatures are obtained for the system interface agreements and the agreements are kept current;

- prepare a comprehensive and complete Y2K contingency plan to address all risks identified in the risk management plan and ensure that all users and key personnel involved in developing the plan are aware of the program status;

- ensure that the functional proponent is kept apprised of changes so that timely actions can be taken and the required attention is focused on the Standard Installation and Division Personnel System 3; and

- establish procedures and a timeline to review and complete the mandatory Y2K certification checklist and ensure that a senior management official grants the certification.

As a response, management stated that the Standard Installation and Division Personnel System 3 had no significant Y2K risks. The major risk was that the Standard Installation and Division Personnel System 3 constituted the Y2K solution of the Army for personnel management and was to be fielded and

operational before the Y2K. The Program Executive Office Y2K Project Officer and the Program Management Office were working closely to validate the Standard Installation and Division Personnel System 3 as Y2K compliant and to review the test plan and processes, documentation, audit trails, and results. Additionally, the Program Manager:

- diverted resources to support Y2K planning, reporting, and testing requirements;

- obtained all of the required interface agreements;

- developed a risk management plan and was scheduled to complete a contingency plan; and

- prepared a fielding plan and made it available to the user community.

Report No. AA 98-176, "Automated Information Systems Year 2000 Army Training Requirements and Resources System," March 30, 1998. The report states that potential risk areas existed and could impact the Y2K compliance of the Army Training Requirements and Resources System. As a result, the potential risk areas required increased management attention. Also, the database submission was generally accurate but had discrepancies with information related to interfacing systems and compliance cost data elements. A review of the Y2K Implementation Plan identified that the plan did not completely address nor did personnel prepare other key strategic plans such as risk management, test, and contingency plans to ensure Y2K compliance. Further, responsible personnel had not signed memorandums of agreement and had not developed test plans for all systems.

Responsible personnel within the Office of the Deputy Chief of Staff for Personnel did not have all the Y2K system interface agreements prepared and signed between the Army Training Requirements and Resources System and all its interfacing systems. The Army Training Requirements and Resources System interfaces with Army and non-Army systems. The report states that because of the number of interfaces, interfaces could have a material impact on Y2K compliance for the Army Training Requirements and Resources System and all of its interfaces if the personnel do not get the agreements developed, documented, and signed in a timely manner.

The report made the following suggested actions to the Army Training Requirements and Resources System Program Manager:

- develop a comprehensive risk management plan,

- develop a comprehensive contingency plan,

- establish a new suspense date to have all memorandums of agreement completed and signed, and

- develop a comprehensive test plan for the Army Training Requirements and Resources System.

The Office of the Deputy Chief of Staff for Personnel stated that the report referred to interfacing agreements as high risk, but the Office considered the risk to be moderate. Also, the Office of the Deputy Chief of Staff for Personnel stated that it had a good handle on the status of interfaces. Additionally, the Office of the Deputy Chief of Staff for Personnel performed some risk analysis and contingency planning but stated that it had not formalized any documentation because it did not want to waste time or effort on a formal document that would need to be redone as the result of a revision to the plan.

Report No. AA 98-175, "Automated Information Systems Year 2000 for the Automated Instructional Management System-Redesign (AIMS-R), March 26, 1998. The report states that the Automated Instructional Management System-Redesign was on target for meeting its Y2K timeline. Personnel were completing or finalizing actions and documentation required to meet the Army Y2K program. The program manager developed a comprehensive risk management and contingency plan. As a result of the risk management plan, the program manager developed the following: a configuration management plan, a quality assurance plan, a test and evaluation master plan, an integrated logistics support plan, a training plan, and a security plan. The report made no suggestions.

Report No. AA 98-107, "U.S. Army, Europe, and Seventh Army's Year 2000 Action Plan," March 3, 1998. The report states that the overall management of the Y2K program of the U.S. Army Europe and Seventh Army was generally effective. The U.S. Army Europe and Seventh Army had developed a Y2K action plan; however, it could have improved its overall management if Department of the Army-level functional proponents provided more guidance and emphasis to the U.S. Army Europe functional components regarding Y2K compliance. Further, the functional proponents viewed the Y2K crisis as an information management problem and, therefore, limited their involvement. The functional proponents did not make Y2K responsibilities a primary duty.

The report states that the Army Y2K database did not accurately portray the status of all the critical systems of the U.S. Army Europe and Seventh Army. The functional proponents misclassified and excluded their systems. Additionally, the U.S. Army Europe did not provide accurate or complete information for most of the key data elements. During the audit, U.S. Army Europe updated the Y2K database to include the inaccurate or missing data, which gave it a baseline to track the Y2K status for its critical systems.

The report states that the U.S. Army Europe and Seventh Army functional proponents did not prepare most of the required Y2K planning and coordination documents, such as strategic plans and contingency plans. The documents that the functional proponents prepared were not comprehensive or complete.

The report suggested that the U.S. Army Europe and Seventh Army require functional proponent points-of-contact to coordinate with system and technical

experts for each unique system to ensure accuracy of database updates. Additionally, the report suggested that the U.S. Army Europe and Seventh Army require the functional proponents to:

- brief Y2K compliance status of their unique systems at Chief of Staff meetings and

- develop, document, update, and maintain strategic plans for critical unique systems to include interface agreements and plans of risk management, testing, and contingency.

Finally, the report suggested that the U.S. Army Europe and Seventh Army make use of available program management software to track the progress of Y2K compliance for each of its critical systems.

Report No. AA 98-122, "Standard Army Retail Supply System Year 2000," February 25, 1998. The report discusses the management structure for Y2K compliance and states that an adequate structure for managing Y2K compliance was developed. The Army Y2K database accurately reflected the status of the Y2K effort for the Standard Army Retail Supply System. Further, the Army drafted a detailed risk management plan and a contingency plan. Also, personnel coordinated with managers of interfacing systems to prepare and sign interface agreements in accordance with the Department of Army October 1996 draft Y2K Action Plan. However, the report includes suggested actions for updating the contingency plan and agreements with managers of interfacing systems according to the January 1998 revised Y2K Action Plan of the Army. The suggested actions directed to the Standard Army Retail Supply System Product Manager were as follows:

- update the draft contingency plan to reflect specific risks identified during the risk assessment process and based on the Army January 1998 revised Y2K Action Plan and

- revise agreements with managers of interfacing systems according to the Army January 1998 revised Y2K Action Plan.

The Product Manager agreed with the findings and stated that the draft contingency plan and the interface agreements would be updated according to the Army January 1998 revised Y2K Action Plan.

Report No. AA 98-128, "Automated Information Systems Year 2000 Global Command and Control System-Army," February 24, 1998. The report states that the Global Command and Control System-Army Y2K progress had been overstated in the October 1997 database submission. During the same time frame, the Army had not completed an inventory of its systems and lacked a comprehensive contingency plan, written interface agreements, and accountability of all interfaces. However, during the audit, the project manager agreed to complete the tasks. The report suggested additional actions as follows:

- make sure that the Y2K plan is revised to ensure correction of any Y2K problems before December 31, 1998, and if not, then report that the system would not meet the December 31, 1998, Y2K target date;

- revise the contingency plan to address the worst-case scenarios; and

- ensure that the project manager or the responsible official for each system interfacing with the Global Command and Control System-Army agrees in writing with all agreements made on system interfaces.

According to the project manager's office, the office would not replace its current software release. Instead, the office would perform a software modification to correct Y2K faults.

Report No. AA 98-127, "Automated Information Systems Year 2000 Advanced Field Artillery Tactical Data System," February 24, 1998. The reports states that the Y2K progress for the Advanced Field Artillery Tactical Data System was overstated. In addition, responsible personnel had not developed interface agreements for 28 systems that interfaced with the Advanced Field Artillery Tactical Data System but had developed a common standard for documenting Y2K compliance of its interfaces. The review raised concerns regarding the lack of Y2K decision and planning documents. As a result, the responsible personnel provided documentation supporting the Y2K status of the system. However, the contingency plan lacked definition for the priority of the Y2K solutions. Also, program personnel stated that obtaining interface agreements was not practical and said that they would not enforce the requirement. Instead, the program personnel agreed to prepare a fact sheet showing standards and specifications for each interface. Suggested actions to the Advanced Field Artillery Tactical Data System Project Manager were as follows:

- monitor any delay in system fielding and ensure that the retrofit decision is made before the trigger date and

- make sure that the project manager or responsible official for each system interface agrees in writing with the details of the agreement regarding system interfaces.

The Advanced Field Artillery Tactical Data System Project Manager did not agree with the report, stating that the report inaccurately stated the facts and projected an unfair negative perception of the Y2K progress. Further, the Project Manager stated that the sole basis of the report was that the project office had not completed the assessment phase documentation the exact date that the renovation phase started. Because no requirement stated that the exit criteria be completed before progressing to a later phase, the project manager stated that the Army Audit Agency should not have had any negative findings.

The Army Audit Agency responded by stating that the Command did not address the suggested actions. In addition, the Army Audit Agency stated that the organization's comments about the progression to a later phase while completing a previous phase is true but misleading. Accordingly, the Army Audit Agency responded that the command's action plan required the completion of the assessment phase by March 31, 1997; however, the audit work began in October 1997, 6 months later. As a result, the critical exit criteria for the assessment phase had not been prepared.

Report No. AA 98-118, "Automated Information Systems Year 2000 U.S. Army Training and Doctrine Command," February 19, 1998. The report discusses the adequacy of the Army Y2K Action Plan to ensure that all mission-critical systems would be Y2K compliant in terms of contingency options and cost at the Army Training and Doctrine Command. The report states that specific management oversight of the Reception Battalion Automated Support System needed improvement. The report shows that problems existed with the accuracy, updating, and completeness of the database. Further, the Army Training and Doctrine Command had not prepared or completed planning and coordination documents such as the contingency plan, test plans, and interface agreements. The suggested actions to the Commander, Army Training and Doctrine Command, were as follows:

- establish procedures to make sure that only personnel knowledgeable of automated systems management were appointed to the position of program manager;

- have the command's Y2K project officer provide written instructions emphasizing the development of risk management plans, contingency plans, test plans, and interface agreements;

- make sure that the database included all mission-critical systems and information regarding the existence of contingency plans and that the exit criteria were completed before moving the system into the next phase, updates were made to the system, and input was required from managers regarding quarterly updates including documentation to support the system status;

- have all responsible management officials monitor the fielding of the systems to make any adjustments needed to accelerate actions or minimize slippages;

- prepare an overall program management program, risk management plan, and contingency plan;

- prepare a test plan for testing migration systems that were fielded; and

- identify all interfacing systems and prepare interface agreements to cover the Y2K issues with the system owners.

Management concurred with all the suggested actions.

Report No. AA 98-115, "Automated Information Systems Year 2000 Forces Command," February 19, 1998. The report states that Forces Command established an adequate management structure and processes to manage the Y2K problem. However, the database information was inaccurate because of input errors. Also, Forces Command could not complete external interface testing until interface agreements were in place for its systems. Although Forces Command had developed contingency plans, the command could not complete the plans until all other interfacing systems were tested. The report recommended that the Forces Command reissue guidance directing the program managers to ensure that external system interface agreements were established, signed, and in place for all interfacing systems.

Report No. AA 98-120, "Automated Information Systems Year 2000, Forward Area Air Defense Command and Control System," February 13, 1998. The report states that the Forward Area Air Defense Command and Control System Y2K progress had been overstated. Documentation was lacking to support the management phase reported for the system. Also, personnel had not performed testing to confirm certification compliance. More importantly, personnel did not view Y2K as a top priority because they perceived it to pose a minimal threat to the system. As a result of the minimal threat assessment by management, the contingency plan did not provide any alternative options for Y2K.

Memorandum Report No. AA 98-116, "Year 2000 Assist-Korea," February 11, 1998. The Eighth Army could have enhanced its Y2K progress in identifying critical systems and in committing appropriate resources to make cost-effective compliance corrections by having organizations prepare required documentation. The Eighth Army input to the Army Y2K database did not include 24 reportable systems. The data elements for the 11 Eighth Army systems included in the Army Y2K database reflected inaccurate data. The Eighth Army could not furnish reliable estimates of the resources needed to make cost-effective corrections for Y2K compliance. The Eighth Army did not enter the cost estimates that it developed during the awareness phase into the Army Y2K database. Additionally, the systems remained in the assessment phase more than 2 months after the Army Y2K deadline to complete the phase, and the Eighth Army did not report the reasons that the systems were still in the assessment phase, as required by Congress and the Office of Management and Budget. Finally, the Eighth Army could not furnish evidence that testing plans were comprehensive and complete and that its organizations developed adequate contingency plans. The report states that the Eighth Army had a highly effective Y2K Management Plan. However, the functional proponents had not seen the plan and needed guidance to implement it. The Army Audit Agency briefed the Acting Assistant Chief of Staff for Information Management and suggested that the Eighth Army include all identified systems in the Army Y2K database, furnish the Eighth Army Y2K Management Plan to the proponents, and require the proponents to submit certification documentation on each system. Additionally, the Eighth Army should require a General Officer or Senior Executive Service level signature for critical systems and an O-6 level signature for all other systems.

The report suggested that the Eighth Army include all identified systems and migration systems that were to replace identified systems in the Army Y2K database and include reliable estimates of resources needed to make the systems Y2K compliant. Further, the report suggested that the Eighth Army prepare reports required by Congress and the Office of Management and Budget explaining the reasons why systems remained in the assessment phase more than 2 months after the Army deadline. The report also suggested several actions for certification. Specifically, the Eighth Army was to take the following actions:

- require proponents of identified systems to prepare and submit required certification documents signed by appropriate certifying officials,

- evaluate certification documents for accuracy and completeness and provide appropriate guidance to functional proponents,

- use certification documents as the basis for input to the Army Y2K database, and

- evaluate certification documents for adequacy of testing plans.

Finally, the report suggested that the Eighth Army evaluate completed Y2K compliance checklist documents for adequacy of contingency plans.

Report No. AA 98-100, "Year 2000 Audit Status Update to LTG William Campbell, Director of Information Systems for Command, Control, Communications, and Computers," January 23, 1998. The report discusses the assessment of Army progress in managing, monitoring, and resolving its Y2K problem. Although the Army was making progress, the report cites improvements to enhance management of the Y2K program. The report suggested the following actions:

- issue a directive requiring the functional proponents to actively engage in enforcing oversight, management, and execution responsibilities as prescribed in the Army Y2K Action Plan;

- require the functional proponents to provide the Chief Information Officer with a signed report outlining the methodology for implementing the Army Y2K Action Plan;

- issue a directive signed by the Chief Information Officer requiring data elements for critical systems to be baselined before activation of the Army Y2K web database;

- require the organizations responsible for making mission-critical systems Y2K compliant to intensify efforts in establishing memorandums of understanding for system interfaces, reporting and resolving issues that impact testing efforts, and developing contingency plans; and

- require addressees of Y2K reports to provide written responses on the resolutions planned for issues identified.

The Army Chief Information Officer directed that immediate action be taken to ensure that no critical system failures result within the Army from Y2K.

Report No. AA 98-36, "Automated Information Systems (Phase I)-Year 2000," January 21, 1998. The report is an assessment of the Department of the Army oversight and management Y2K effort. Results indicate that points of contact within the functional proponent areas could not adequately articulate the implementation procedure for their Y2K responsibilities. Only 1 of the 10 functional proponents could adequately ensure that Y2K had been a top priority of the proponent. Also, the Army Y2K database did not provide accurate or complete information needed to centrally manage and oversee the planning, monitoring, and resolution of the Army Y2K efforts. The report suggested that the functional proponents become more actively engaged in executing the Y2K oversight programs. Also, a concerted effort was to be made to baseline the Y2K database to improve its use in managing and reporting the status of the Y2K

program. Management generally agreed with the following suggested actions addressed to the Director of Information Systems for Command, Control, Communications, and Computers:

- issue a memorandum requiring functional proponents to become actively engaged in enforcing their oversight management and execution responsibilities as prescribed in the Army Y2K Action Plan and

- require functional proponents to report what they are doing to implement the jointly signed memorandum in routine meetings chaired by the Director of Army Staff and the Under Secretary of the Army.

Inspector General, Navy

"Report of Y2K Assessment of the Commander Naval Reserve Force," October 15, 1998. The report states that the Inspector General, Navy, conducted an assessment of the Commander Naval Reserve Force in the areas of personnel management, planning and operations training, logistics and facilities, communications and information and technology infrastructure, and financial management. The report concludes that the Commander Naval Reserve Force was still in the assessment phase because of the large number of facilities and structures that remained to be evaluated and inventoried. Also, some mission-critical systems did not have the required contingency plans, nor did continuity-of-operations plans or Y2K management plans exist. For systems that had contingency plans, the report states that the plans had not been tested. Although personnel at the Commander Naval Reserve Force had confidence that the disaster recovery plans would handle the Y2K problems, the report states that the Inspector General, Navy, staff did not share that same level of confidence. In addition, the report states that the time period between the systems validation date, November 30, 1998, and the implementation date, December 31, 1998, was too short and would not ensure the completion of the systems implementation process. Also, nontechnical functional area directors did not participate in assessing the Y2K problems that could impact their systems. The Commander Naval Reserve Force had to absorb the costs out of its operating budget. Further, little training had been provided to assist the nontechnical functional area directors in assessing Y2K risks. The documentation to support the memorandums of agreement, contingency plans, and continuity of operations was not reconcilable with the information maintained within the Navy Y2K database. Also, the command did not prepare integrated test plans to ensure operability of the telecommunications service, so the possible risks and disruptions were unknown. The recommendations to the Commander Naval Reserve Force included the following:

- take steps to get middle-level nontechnical functional leadership fully engaged in managing Y2K and developing reliable contingency plans and continuity-of-operations plans;

- review the implementation schedule and adjust it as required;

- have functional leaders review the Y2K problem and determine the impact;

- direct functional area personnel to ensure that mission functionality be maintained in accordance with the system plan;

- ensure that all subordinate levels are consistently engaged in Y2K efforts;

- develop and promulgate telecommunications guidance regarding service outage or degradation risks associated with Y2K problems;

- work with the Defense Information Systems Agency in determining Y2K risks with DoD and Navy long-haul telecommunications services and distribute the information to all Navy commands;

- provide appropriate Y2K training, policy, and guidance to lower echelon commands; and

- complete and execute test plans to ensure that the system is Y2K compliant as required by contract.

"Review of Echelon II Year 2000 Programs," July 8, 1998. The report states that Navy components were not treating Y2K as a high priority or as a business problem. In many commands, top-level business managers were not involved in, aware of, nor supportive of Y2K efforts. As a result, the Navy Y2K problem was underreported. Because of the confusion of what constituted a "mission-critical" system, Navy components did not report some critical business applications or roll the critical business applications into one for reporting purposes. Exit criteria were not clearly defined, and documentation was not required to verify the phase transition allowing each command to define its own criteria for phase completion. As a result, the Navy components inaccurately reported the phase status of the systems. The inventory data were incomplete, and interfaces had not been completely identified. Also, Navy components had no consistent assessment methodology, and system ownership was not well-defined. Further, the Navy Action Plan required that the Navy components complete the compliance checklist and provide a copy to the command's Y2K coordinator, but few checklists had been completed. Commands could not perform mainframe testing because the Megacenters' equipment was not Y2K compliant. In addition, application testing was not part of the annual fee that commands pay to the Defense Megacenter that provided the service on a fee-for-service basis. As a result, commands would require additional funding for which commands did not program. A plan for testing requirements for the commands had not been developed. Guidance and assistance to commands from higher echelons was not provided effectively. Because of those issues, the memorandum concludes that the Navy was behind in its Y2K effort. Additionally, the scope of the Y2K problem of the Navy was unknown, and the same was true of the Y2K progress of the Navy. Navy leaders had not perceived the impact that Y2K could potentially have on readiness. The report concludes that the Navy had no sense of urgency to resolve the Y2K issue, which was disturbing because of the time limitation to resolve Y2K issues. The report contains no recommendations.

Naval Audit Service

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Air Systems Command, Program Executive Office for Tactical Aircraft Programs, October 9, 1998. The memorandum states that the Program Executive Office for Tactical Aircraft Programs (the Program Executive Office), Naval Air Systems Command, was in the validation phase of its Y2K program. Also, the memorandum states that the Naval Audit Service believed that additional resources should be committed to the Y2K efforts for developing contingency plans and ensuring completion of memorandums of agreement. On June 29, 1998, the Navy issued expanded guidance for contingency plans requiring all mission-critical items to have operational contingency plans by December 31, 1998. However, the Program Executive Office did not identify and report all of its Y2K costs. Further, the Program Executive Office had not finalized all of its memorandums of agreement or its Y2K Action Plan. As a result of the review, the Naval Audit Service noted discrepancies between the information reported in the Navy Y2K database and the information reported by the program managers. The memorandum recommended that the Program Executive Office take the following actions:

- develop, document, and test realistic contingency plans in accordance with the Navy June 29, 1998, guidance;

- track all Y2K costs where applicable for reporting purposes;

- report the results of the outstanding memorandums of agreement to the Command by October 31, 1998;

- develop a formal Y2K Action Plan; and

- establish a reconciliation process to reconcile the information reported by the program managers with the data reported to the Navy Y2K database.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Sea Systems Command (Team CX), September 18, 1998. The Naval Sea Systems Command Program Executive Office for Expeditionary Warfare and the Program Office for Carriers are collectively called the Naval Sea Systems Command Team CX. Overall, the memorandum states that the Team CX was in the assessment phase. Based on the results of the Naval Audit Service review, Team CX would not meet its implementation target dates. The memorandum states that Team CX had not accurately tracked and reported the ship platforms and major systems. Consequently, the Y2K status reported was incorrect and did not accurately represent the Y2K progress of Team CX. Also, the contracts awarded by Team CX did not contain the appropriate Y2K language. Additionally, the Y2K costs were not requested, tracked, nor reported in accordance with the Navy Chief Information Officer guidance. The program office for 3 mission support systems had not obtained interface agreements and had not provided completion of testing documents. Furthermore, Team CX had not completed its assessment of the

infrastructure and had not reported all interfaces to the Navy Y2K tracking system nor had it obtained all of the memorandums of agreement. The memorandum recommended that Team CX:

- report the ship platforms and major systems into the Navy Y2K database and place them in their appropriate phase;

- review all current and future contracts to ensure inclusion of Y2K contract language;

- prepare and submit contingency plans in accordance with the Navy Chief Information Officer guidance for all systems and ship hulls that were not currently in validation or would not be implemented by December 31, 1998;

- develop a method to track Y2K costs in accordance with the Navy Chief Information Officer guidance;

- identify and report all system interfaces into the Navy Y2K database;

- obtain signed memorandums of agreement for all required system interfaces; and

- complete the infrastructure assessment and report the results to the Navy Chief Information Officer.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Program Executive Office for Theater Air Defense and Surface Combatants, Naval Sea Systems Command, September 18, 1998. The memorandum states that the Naval Audit Service performed two evaluations at the Naval Sea Systems Command, one of the systems and another of the ship platforms. Based on the evaluations, the memorandum states that the Naval Sea Systems Command would not meet its implementation target completion dates. Overall, the Command had not reported the ship platform systems in the Navy database, did not accurately represent its Y2K progress, and had not included the Y2K contract language in all the contracts. Also, all system interfaces had not been identified nor had the infrastructure items been properly reported in the Navy database. Further, all Y2K costs had not been reported. The memorandum recommended that the Naval Sea Systems Command accurately report ship platforms or major systems in the Navy Y2K tracking system database. The report also recommended that the Program Executive Office:

- update information to accurately report the Y2K progress or work remaining to be accomplished for Y2K issues,

- review current contracts to ensure inclusion of Y2K language and review all contract warranties to ensure that the manufacturer liability would not be negated for Y2K compliance because the required language was missing,

- identify and report all system interfaces to the Navy Chief Information Officer,

- remove information technology infrastructure items from the Navy Y2K database and report them as infrastructure items, and

- develop a method to track and report Y2K costs.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Program Executive Office for Air Anti-Submarine Warfare, Assault, and Special Mission Programs, Naval Air Systems Command, September 17, 1998. The memorandum states that the Naval Air Systems Command, Program Executive Office for Air Anti-Submarine Warfare, Assault, and Special Mission Programs (the Program Executive Office) needed to commit additional resources to the Y2K initiative. The Program Executive Office needed the additional resources to improve its development of contingency plans, to assist in the completion of the renovation phase, and to maintain the required Y2K documentation. As a result of the need for additional resources, the Program Executive Office had not identified all Y2K costs in the database nor completed all of its memorandums of agreement. Also, discrepancies existed between the information maintained by the program managers and the information reported in the Navy Y2K database. Furthermore, the Program Executive Office did not have adequate documentation for the solutions to the Y2K problems identified. Additionally, the Program Executive Office awarded a contract that did not contain the Y2K contract language required by the Federal Acquisition Regulation. Finally, the Program Executive Office needed guidance for reporting systems in development that were expected to be delivered after Y2K. The memorandum recommended the Program Executive Office:

- track all Y2K costs and report the costs to the Navy database,

- pursue the completion of memorandums of agreement,

- reconcile information reported by the command with the information reported in the database,

- ensure that documentation exists to adequately support the remedies identified for Y2K solutions, and

- comply with the requirement of the Federal Acquisition Regulation.

The memorandum recommended that the Naval Air Systems Command identify and report production equipment owned and managed by the Air Anti-Submarine Warfare, Assault, and Special Mission Programs. The memorandum also recommended that the Navy Chief Information Officer develop guidance to clarify the issue of systems in development to ensure Y2K compliance of all mission-critical systems.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Navy Undersea Warfare, August 28, 1998. The memorandum states that the Navy Undersea Warfare Program Executive Office is in the renovation phase and had certified a total of 135 systems. However, the Naval Audit Service stated that it did not agree with the certification process of the 135 systems. Further, the Navy Undersea Warfare Program Executive Office did not report its Y2K strategy for repairing and resolving Y2K problems in the Navy Y2K tracking system as required. Also, the Navy Undersea Warfare

Program Executive Office included Y2K costs with other system enhancements, making it difficult to sever, identify, and report only the Y2K costs. Finally, the Navy Undersea Warfare Program Executive Office had not identified all interfaces and had not developed and documented all of its test plans. The memorandum recommended that the Navy Undersea Warfare Program Executive Office do the following:

- follow the Navy Chief Information Officer Action Plan dated April 1998 and the guidance related to system certification;

- report the Y2K strategy as required by the Navy Chief Information Officer Action Plan dated April 1998;

- report direct costs related to resolving Y2K;

- ensure that new desktop, laptop, and fax machine contract purchases contain language stating the purchases are Y2K compliant;

- identify all system interfaces and complete all memorandums of agreement; and

- ensure that test and implementation plans were in place and documented and prepare contingency plans for all mission-critical systems by December 31, 1998.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval War College, August 26, 1998. The memorandum states that the Naval War College was in the assessment phase and did not have any reportable systems. However, the college reported two local area networks that it should have included in the data collected for the information technology infrastructure. As a result, the college had not fully assessed its information technology infrastructure nor had the college inventoried its facility infrastructure or its local unique information systems. In addition, the college did not identify all of its interfaces. The memorandum recommended that the Naval War College take the following actions:

- inventory all categories of infrastructure assets as outlined in the Navy Chief Information Officer Action Plan and

- identify all interfaces and obtain memorandums of agreement for all interfaces.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Operations Naval Support Activity, August 26, 1998. The memorandum states that the Operations Naval Support Activity did not have any mission-critical systems but did have a mission-support system and one database. However, the activity provided software and hardware procurement and maintenance support to its users located at various temporary and permanent sites. An initial review showed that the Operations Naval Support Activity did not address the uniqueness of the user systems and did not meet the target date for completing the systems assessment phase. Also, the information regarding the inventory of systems and system interfaces was either incomplete or inaccurate. Further, the activity did not develop contingency or test plans. The

memorandum made recommendations for the assessment, renovation, and validation phases of the Operations Naval Support Activity Y2K Program. The memorandum recommended that the Operations Naval Support Activity accomplish the following:

- contact the Navy Chief Information Officer to determine how to report the Y2K inventory and ensure that the inventory was reported in the Navy Y2K database;

- provide a complete inventory of all systems and report the information to the Navy Y2K database by September 30, 1998;

- identify all interfaces and finalize memorandums of agreement by September 1998;

- provide memorandums of agreement status with major DoD activities to the Navy Chief Information Officer;

- perform an inventory of infrastructure items with embedded chips;

- prepare programmatic and operational contingency plans in accordance with the Navy Chief Information Officer; and

- continue pursuing funding for the operating system upgrade and establish a testing schedule for the database.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," United States Naval Academy (USNA), August 26, 1998. The memorandum concludes that the Naval Academy had four mission-critical systems and that the systems would be replaced. Also, the Naval Academy considered the systems to be in the renovation phase. However, the memorandum discusses other issues that required the attention of management and made recommendations for Y2K improvements. The memorandum recommended that the Naval Academy accomplish the following:

- refine its corporate strategy and activity plan for handling the Y2K problems to include non-mission-critical systems and infrastructure items,

- complete an assessment of infrastructure categories,

- develop a contingency plan for the replacement effort, and

- conduct independent testing and certification of all systems.

Also, the memorandum states that the academy should commit additional resources to solve the Y2K problems and meet DoD and the Department of the Navy Y2K deadlines. The academy reported that the replacement cost for the telephone switches would be $1.3 million.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Strike and Air Warfare Center (NSAWC), August 24, 1998. The memorandum states that the Naval Strike and Air Warfare Center had no reportable Y2K systems but did have four categories of shore infrastructure systems, devices, and infrastructure to be reported. According to the review conducted, the Naval Strike and Air Warfare Center was in the assessment phase of the five-phase management process The inventory was incomplete for the infrastructure and mission-support systems. The Naval Strike and Air Warfare Center did not document issues raised in the users group or designate Y2K points of contacts within the departments. Also, the center did not report its inventory information to the overall Navy Y2K tracking system. Finally, the Naval Strike and Air Warfare Center did not assess all systems for Y2K compliance and develop contingency plans to ensure continued operations in the Y2K. The memorandum recommended that the Naval Strike and Air Warfare Center accomplish the following:

- inventory all categories of infrastructure assets as outlined in the Chief Information Officer Action Plan of the Navy;
- appoint Y2K points of contact;
- conduct bimonthly Y2K meetings and disseminate Y2K strategies and guidance;
- provide the proper forms and needed passwords for entering data into the Navy Y2K Tracking System;
- assess systems and infrastructure for Y2K compliance;
- require major commands to distribute Y2K system status to all end users;
- test hardware to ensure Y2K compliance;
- ensure Y2K compliance to continue functionality of the fleet; and
- develop, document, and test realistic and reasonable contingency plans for continued operations.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Space and Naval Warfare Systems Command (SPAWAR), August 24, 1998. The memorandum states that the Space and Naval Warfare Systems Command was at risk of not meeting the required DoD and Department of the Navy Y2K target completion dates. The major risks were as follows:

- the time needed for testing and certification,
- the time required to field Y2K compliant hardware and software, and
- the availability of the fleet implementation.

Also, reporting efforts of the systems inventory were inconsistent with the overall Navy tracking systems database. Furthermore, the Space and Naval Warfare Systems Command certified systems without identifying all of the system interfaces. As a result of the review, management might have needed to commit additional resources to obtain memorandums of agreement and complete laboratory testing before meeting the Y2K target completion dates. The memorandum recommended that the Space and Naval Warfare Systems Command accomplish the following:

- ensure that Y2K status receive the widest distribution,

- refine corporate strategy and the action plan for handling the Y2K initiative to include the Space and Naval Warfare Systems Command System Center Information Technology Infrastructure items,

- reconcile the database information reported as input for the Navy tracking system database and resolve password problems with the Navy tracking system database,

- become more aggressive in getting memorandums of agreement signed and identifying system owners before certifying any system's Y2K compliance,

- track all Y2K costs for reporting purposes and ensure that contingency plans are realistic and reasonable,

- schedule and prioritize mission-critical systems testing to ensure that the fleet implementation schedule is met,

- coordinate with the commands of other systems to escalate installation of hardware and software at the fleet, and

- correct erroneous information reported about the system status.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Program Executive Office (Team Submarine), Naval Sea Systems Command, August 13, 1998. The memorandum states that the Naval Sea Systems Command, Program Executive Office (Team Submarine) was in the assessment phase of its Y2K program. However, the command was at risk of not meeting the target completion date for the implementation of Y2K. The Naval Sea Systems Command did not adequately report the ship platforms or ship hull numbers on the Navy Y2K database. Further, the Program Executive Office (Team Submarine) did not evaluate system interfaces for Y2K issues. Overall, the Y2K progress of Team Submarine was overstated, as shown in the following examples:

- most systems certified as Y2K compliant included systems with no Y2K issues,

- data related to reporting all infrastructure items (including the ship platforms) had not been reported within the Navy database,

- memorandums of agreement had not been completed for all system interfaces, and

- contingency plans had not been completed in accordance with Navy guidance for Y2K.

The memorandum recommended that the Naval Sea Systems Command report the ship platforms to ensure that the database was accurate. The memorandum also recommended that the Program Executive Office (Team Submarine):

- reflect the actual remaining work by not including systems with no Y2K issues;

- establish goals with a plan of action to ensure completion of system inventories, database updates, memorandums of agreement, and contingency plans in accordance with deadlines imposed by Navy guidance;

- periodically reconcile the status of the system inventory and include an inventory of the infrastructure; and

- direct personnel to prepare programmatic and operational contingency plans in accordance with Navy guidance.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Sea Systems Command (NAVSEA) for Mine Warfare, August 7, 1998. The memorandum concludes that the Naval Sea Systems Command for Mine Warfare did not document any risk assessments that it performed, nor did it complete the assessments of the information technology infrastructure items, identify interfaces, and execute memorandums of agreement. Additionally, the command did not accurately report the number of compliant systems and did not track Y2K costs to ensure the availability of funding for the completion Y2K requirements. As a result, the memorandum recommended that the Naval Sea Systems Command for Mine Warfare accomplish the following:

- develop, document, and distribute an organization Y2K risk assessment plan;

- refine corporate strategy for handling the Y2K initiative to include information technology infrastructure items;

- contact the system owners of external interfaces to determine compliance status and whether memorandums of agreement were needed;

- develop contingency plans, especially for systems not expected to meet the implementation target date, to include training on expectations after Y2K;

- track Y2K costs; and

- conduct Y2K independent testing and certification for systems requiring Y2K corrections and certify only those systems meeting the certification requirements or justify those that are certified noncompliant but acceptable.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Safety Center (NAVSAFECEN), August 7, 1998. The memorandum states that the Naval Safety Center provided a preliminary inventory of systems to assess its Y2K progress. The Naval Safety Center did not report its inventory to the Navy Chief Information Officer because it initially reported the inventory through the Defense Integration Support Tools database. The Naval Safety Center did not establish memorandums of agreement for the majority of the interfaces identified, and Naval Safety Center personnel were unsure whether interfaces with major DoD systems needed to be identified in the Navy inventory of interfaces. Further, the Naval Safety Center did not develop contingency plans and did not complete the certification process for the systems identified as Y2K compliant. Also, the Naval Safety Center had not performed an inventory to identify embedded chips. As a result, the memorandum recommended that the Naval Safety Center apply for a password to input inventory data into the Navy Chief Information Officer database, finalize memorandums of agreement using the Navy guidance and provide the status to the Navy Chief Information Officer, include interfaces with major DoD systems in accordance with the Navy Chief Information Officer guidance, develop realistic contingency plans for those systems for which they were needed, review certification requirements and obtain a signed certification document for each system determined to be Y2K compliant, and perform an inventory of embedded chips.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Commander Naval Legal Services Command (CNLSC), August 7, 1998. The memorandum states that the Commander Naval Legal Services Command was in the validation phase and would meet the implementation target completion date of the Navy. The field activities of the Naval Legal Services Command did not designate Y2K points of contact, leaving the Y2K personnel at the headquarters level responsible for managing all the activity's Y2K efforts. The command did not report any of its systems in the Y2K database of the Navy because the personnel did not have access to the database or feel that the systems at the Commander Naval Legal Services Command met the definition outlined in the Navy Chief Information Officer's guidance. The Commander Naval Legal Services Command used the Navy Chief Information Officer's Information Technology Standards Guidance to determine whether the hardware and software were Y2K compliant but did not perform testing. Also, the Commander Naval Legal Services Command placed systems in the implementation phase without meeting the certification requirements for Y2K compliance. The memorandum recommended that the Commander Naval Legal Services Command designate Y2K points of contact at the field activities. Also, the memorandum recommended that the Navy Chief Information Officer provide a password so that personnel could update the database. Finally the memorandum recommended the Navy Chief Information Officer provide guidance on the appropriateness of using the Information Technology Standards Guidance to determine Y2K compliance without testing and require that certification documentation be prepared to support all systems reported as Y2K compliant.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," President Board of Inspection and Survey (PRESINSURV), July 15, 1998. The memorandum states that the President Board of Inspection and Survey had not coordinated with other components to ensure that software programs had been included in the inventory. Also, the President Board of Inspection and Survey was not included on the Navy Chief Information Officer distribution list and had not reported any system data. The President Board of Inspection and Survey was to replace and test existing computers by October 1998. Further, the President Board of Inspection and Survey certified 85 percent of the 300 identified systems as completed. The President Board of Inspection and Survey had not determined the facilities to be Y2K compliant and had not tracked Y2K costs. As a result, the memorandum recommended that the President Board of Inspection and Survey accomplish the following:

- coordinate with other components to ensure that all unique software programs were identified in the overall inventory of all information technology items,

- obtain a password for the Navy database and provide the complete inventory of all systems,

- ensure that the appropriate Y2K contract language was included in the purchase request for the new computers,

- review certification requirements and obtain signed certification documentation for each system determined to be Y2K compliant,

- review the guidance of the Navy on infrastructure and determine whether facilities are Y2K compliant, and

- track all Y2K costs for reporting purposes.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Commander, Naval Meteorology and Oceanography Command (COMNAVMETOCCOM), July 13, 1998. The memorandum states that the Commander, Naval Meteorology and Oceanography Command, would meet the Y2K target date. The command was in the renovation phase but had not conducted an organizational risk assessment. Further, the command did not track information technology assets adequately. The Command had not established memorandums of agreement for all mission-critical system interfaces. Finally, the command had not documented the systems in the renovation phase. The memorandum recommended that the Naval Meteorology and Oceanography Command develop, document, and distribute an organizational Y2K risk assessment plan in accordance with the Navy Action Plan dated April 1998; redefine the term "system" to ensure that all assets would be uniquely identified and tracked, including those procured from local funds, therefore precluding the likelihood of duplicate reporting; and formally document contingency plans for systems not scheduled to complete the renovation phase.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Commander, Naval Reserve Forces (COMNAVRESFOR), June 22, 1998. The memorandum states that the Commander, Naval Reserve Forces, would not meet the Y2K target date. Overall, the Naval Reserve Forces were in the assessment phase. The command had not established goals, a plan of action, and milestones to ensure the timely completion of the facility and system inventories. The Naval Reserve Forces had not prepared Y2K database updates, memorandums of agreement, and contingency plans in accordance with the deadlines imposed by the Navy Chief Information Officer Y2K Action Plan. The memorandum recommended that the Naval Reserve Forces require the command to develop, document, and distribute an organizational risk assessment plan; request that the Navy Chief Information Officer intercede with DoD to provide Navy customers with isolated Y2K compliant testing environments; establish Y2K memorandums of agreement for Navy interfaces with the DoD systems; and ensure that contingency plans were formally documented.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Chief of Naval Education and Training (CNET), June 12, 1998. The memorandum states that the Chief of Naval Education and Training had not developed a written risk assessment and documented the organizational strategy. Also, the Chief of Naval Education and Training may not have identified all external interfaces and did not prepare contingency plans for all of its systems. The Chief of Naval Education and Training awarded a contract to replace a system, but the contract did not contain Y2K contract language. The memorandum recommended that the Chief of Naval Education and Training:

- formalize and disseminate an organizational Y2K strategy and refine the corporate strategy for handling the Y2K problems,

- complete the inventory and assessment of non-corporate information technology infrastructure,

- complete the inventory and review external interfaces for completeness and ensure the establishment of memorandums of agreement,

- formally document contingency plans, and

- ensure that the contract was modified to comply with Y2K requirements.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Air Systems (NAVAIR) Command, May 14, 1998. The memorandum states that the Naval Air Systems Command had not disseminated its draft action plan for handling Y2K related issues to all the components. Additionally, the Naval Air Systems Command had not provided database access to each of its organizations, and no schedule had been established for updating the inventory database. Further, the command had not developed guidance to ensure that viable contingency plans would be established for all mission-critical systems. The Naval Air Systems Command was having difficulty establishing memorandums of agreement with external activities. Finally, program managers were interpreting testing and certification differently

and not tracking and reporting Y2K-related corrections adequately. As a result of those issues and concerns, the memorandum recommended that the Naval Air Systems Command take the following actions:

- update, finalize, and distribute the Y2K Action Plan;

- provide each manager with data entry capability to update the centralized database and establish a schedule for updating the centralized database;

- provide clearer guidance for developing contingency plans and ensure that the plans are workable for systems not scheduled to meet milestone dates;

- elevate memorandums of agreement to ensure that they were established and all elements were addressed properly and provide an inventory of DoD system interfaces with a history of attempts to establish and resolve the memorandums of agreement;

- provide clearer Y2K guidance for testing and certification of mission-critical systems and conduct third-party independent testing and certification where applicable; and

- identify and track funds used for Y2K-related problems and report them as accurately as possible.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Historical Center (NHC), May 5, 1998. The memorandum states that the Naval Historical Center managers briefed the Y2K status documented within the report. The Naval Historical Center personnel provided a list of headquarters inventory; however, they could not provide an inventory of the equipment at their detachments. Also, the center was in the process of obtaining memorandums of understanding for each DoD system that it uses. The Naval Historical Center was conducting tests to ensure that the systems would continue to function well after January 1, 2000. The memorandum recommended that the Naval Historical Center accomplish the following:

- update its inventory to include the detachments information and respond to the April 1998 data call because it asks for equipment information not previously requested and

- prepare contingency plans for all equipment that would not be Y2K compliant to ensure that noncompliant systems would provide the functionality needed to process work without disruption.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," U.S. Naval Observatory (USNO), April 21, 1998. The memorandum states that the U.S. Naval Observatory (the Observatory) had long recognized the potential problems for Y2K. Consequently, the Observatory conducted thorough assessments and developed comprehensive action and contingency plans. However, the Observatory negotiated contracts before the issuance of the Navy Chief Information Officer's Y2K guidance. The memorandum recommended that the Observatory provide an update of its Y2K information that was reported to the Navy database, use the web page to

keep users informed of systems' Y2K compliance because the Observatory interfaced with so many users, and adjust the vendor delivery dates and contingency plan trigger dates to comply with the Navy Chief Information Officer's guidance for mission-critical systems. Because congressional guidance gave priority to Y2K issues over scheduled upgrades, the U.S. Naval Observatory was to identify upgrades as Y2K issues to ensure funding.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Field Support Activity (FSA), April 16, 1998. The memorandum states that the Field Support Activity had not appointed a Y2K coordinator or developed a corporate strategy for handling the Y2K problems. The Field Support Activity system inventory data were incomplete, and contingency plans had not been developed for the system scheduled to be replaced. The memorandum recommended that the Field Support Activity formally appoint a Y2K coordinator and develop a corporate strategy outlining its methodology for managing Y2K issues; establish an inventory with milestones and reporting criteria that would include those systems at subordinate commands and infrastructure items; and conduct third-party independent testing and certification for Y2K compliance for mission-critical hardware, non-mission-critical hardware, and embedded chips. The Field Support Activity agreed to commit additional resources to solving its Y2K problems and meeting the Navy deadline.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Navy Tactical Support Activity (NTSA), March 14, 1998. The memorandum states that the Navy Tactical Support Activity provided data for inclusion into the Defense Integration Support Tools database but did not know whether the information was included. Also, the Navy Tactical Support Activity personnel knew about Y2K and indicated that the activity had no Y2K date problems because of enforced programming standards and the design review structure implemented in 1987. The Navy Tactical Support Activity was in the process of documenting and certifying completion of the five-phase management approach. The memorandum recommended that the Navy Tactical Support Activity document that the Y2K issue was adequately addressed in planning so that any potential Y2K problems would be resolved before Y2K.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Naval Supply Systems Command (NAVSUP), March 12, 1998. The memorandum states that the Naval Supply Systems Command had followed the guidance and procedures to complete the command's Y2K process on schedule. However, the Naval Supply Systems Command had not completed memorandums of agreement. Also, the Naval Supply Systems Command only maintained data on the local systems, and the memorandum states that to better track Y2K actions, the command should expand the data request to subordinate commands. The memorandum states that the following results needed to be elevated to the Navy Chief Information Officer: essential assets were still being used in routine sustainment requirements and system enhancements, the inability to use or update the Defense Integration Support Tools database or both was hindering data-gathering efforts and causing interruptions to the reporting requirements, and a decision had to be reached to allow the Naval Supply Systems Command to properly report Y2K actions.

Air Force Audit Agency

Air Force Audit Agency Project No. 98066033, "United States Strategic Command Year 2000 Issues," September 29, 1998. The review was conducted from February through April 1998. Overall, the U.S. Strategic Command was effectively meeting the Y2K program milestones and showed evidence of substantial progress since the program's inception. However, the report identifies that the U.S. Strategic Command Y2K personnel did not properly estimate and report Y2K costs in the Air Force Automated Systems Inventory database. Specifically, personnel did not prepare cost estimates or fully accumulate actual expense data including Y2K overhead costs for any of the 30 systems reviewed. The U.S. Strategic Command did not have a good understanding of cost estimating and reporting procedures under the Y2K program and did not consider such efforts as value added because it did not believe that it would be reimbursed for the costs to make systems Y2K compliant. The report states that preparing good-faith cost estimates and accurately accumulating costs were imperative to fully identify requirements and budget shortfalls.

The report recommended that the U.S. Strategic Command Director for Command, Control, Communications, and Computer Systems direct the Y2K program manager to accomplish the following:

- coordinate with the Air Force Y2K Program Management Office to develop a good understanding of cost estimating and reporting procedures under the Y2K program, to include why such efforts were value added whether or not reimbursements occurred;

- task systems personnel to develop and report required cost data for providing assistance with Y2K program procedures as necessary; and

- monitor cost data inputs for reasonableness and completeness, following up as necessary.

The U.S. Strategic Command concurred with the recommendations and initiated timely actions to correct the issues described.

Air Force Audit Agency Project No. 98066032, "United States Transportation Command Year 2000 Issues," September 25, 1998. The review was conducted from February through April 1998. Overall, the U.S. Transportation Command was effectively meeting the Y2K program milestones and showed evidence of substantial progress since the program's inception. However, the report states that the classified local area network manager did not retain evidence of a thorough system analysis, risk analysis, or contingency plan before reporting that the classified local area network properly completed all assessment phase requirements. Instead, the systems managers used their working knowledge to determine that Y2K would not affect the classified local area network and concluded that they did not need to prepare documentation supporting completion of the Y2K assessment phase requirements. The report states that a thorough system analysis would reduce the risk of hidden data fields and unidentified interface complications. Additionally, a well-documented system analysis would minimize duplicate assessment efforts, reduce resource expenditures, and provide reasonable assurance that responsible personnel

assessed the Y2K impact. Finally, an effective risk analysis, coupled with an appropriate contingency plan, would protect against mission failure and enable the Air Force to perform critical functions in the event of a system crisis.

The report recommended that the U.S. Transportation Command Director for Command, Control, Communications, and Computer Systems direct the Y2K program manager, in coordination with the classified local area network system manager, to document a thorough system analysis, risk analysis, and contingency planning. The U.S. Transportation Command concurred with the recommendations and initiated timely actions to correct the issues described.

Air Force Audit Agency Project No. 98066019, "Management Advisory Service, Phase Status Validation for the Year 2000 Program," June 10, 1998. The review summarizes the results of the review of 20 Air Force activities; the activities are listed in Appendix C of this report. The review assesses the reliability and integrity of Y2K status reporting through the Air Force Automated Systems Inventory. Furthermore, the review states that available data and in-use procedures did not provide reasonable assurance to validate the reported data's reliability and integrity. Specifically, evidence was not available to demonstrate that system managers properly satisfied exit criteria for 348 (68 percent) of the 508 systems reviewed. For the 348 systems, systems managers did not:

- develop or record system analyses, or both, for 116 systems, or 33 percent;
- identify, evaluate, or report interfaces, or any combination of them, for 107 systems, or 31 percent;
- initiate or complete contingency plans, or both, for 165 systems, or 47 percent;
- develop or report cost estimates, or both, for 236 systems, or 68 percent; and
- complete timely database updates for 164 systems, or 47 percent.

Additionally, for 86 of the 508 systems reported in the implementation phase as complete, system managers did not do the following:

- support testing conclusions for 34 systems, or 40 percent;
- complete program checklists for 37 systems, or 43 percent; and
- obtain system certification for 49 systems, or 57 percent.

The report states that the reliability and integrity of Y2K status reporting through the Air Force Automated Systems Inventory did not provide reasonable assurance to validate the reported data's reliability and integrity because of insufficient program emphasis, working groups' agenda, guidance issues, contractor reliance, inadequate attention to data accuracy, and cost data and scope relevance.

Insufficient Program Emphasis. Major Command and center-level management did not always provide adequate support, either through command prioritization or sufficient resources. As a result, personnel issues, such as turnover and full-time duty assignments, were a continuing problem, and working groups did not have either the authority or the inclination to pursue program progress.

Working Groups' Agenda. Working groups at several Major Commands and center locations initiated formal Y2K efforts before the Air Force developed its Y2K program, and the working groups did not later integrate the Air Force requirements into their programs. As a result, system managers did not initiate or complete some critical criteria even while achieving outstanding progress with other significant program requirements.

Guidance Issues. The Major Command and center-level working group focal points and systems personnel responsible for disseminating or implementing Air Force guidance, or both, did not always maintain current guidance or seek clarification when unclear about specific issues. As a result of poorly used and interpreted guidance, costly and timely reanalyzing and retesting may have been necessary for systems improperly declared compliant that were later associated with Y2K problems.

Contractor Reliance. System managers relied on contractor efforts without thoroughly evaluating or monitoring those efforts to ensure compliance with Air Force requirements. As a result, minimal evidence existed that mission-critical and mission-essential systems successfully completed criteria established to reduce the risk that Y2K complications would degrade mission capability.

Inadequate Attention to Data Accuracy. Responsible personnel did not identify Air Force Automated Systems Inventory errors to include inaccurate phase or criticality-level data or line items wrongly identified as systems. As a result, senior managers at all levels were relying on and basing critical resource decisions on persistently erroneous data.

Cost Data and Scope Relevance. Y2K personnel did not always properly develop and report Y2K costs. Specifically, personnel did not accumulate Y2K related cost data, to include personnel, program execution, and equipment. As a result, the Air Force would be unable to reasonably assess the Y2K magnitude or accurately identify critical budget shortfalls.

The Air Force Audit Agency accomplished the review at the request of the Air Force Director, Communications and Information, and accordingly, senior Air Force leaders took substantial positive actions both during and following the management advisory service. Specifically, the Secretary of the Air Force issued a directive memorandum to all Major Commands on Y2K criticality, and the Air Force Chief of Staff included Y2K in a special interest Notice to Airmen. Furthermore, the Air Force Director, Communications and Information, and the Y2K Program Management Office increased efforts to ensure program visibility, to improve data integrity, and to measure Y2K progress. The Y2K program personnel used Air Force-wide publications, directive messages, database improvements, and Air Force-wide working group meetings.

Air Force Audit Agency Project No. 97066036, "Systems Assessment for the Year 2000 Program," May 21, 1998. The report summarizes the audit results of the review of 14 Air Force installations of which 12 installation reports were issued. The reports are listed in Appendix C of this report. The report states that Air Force activities needed to strengthen their Y2K system assessment efforts. Specifically, major command and operating personnel did not always complete system analyses, evaluate system interfaces, prioritize and schedule system renovations, or initiate contingency operations plans. Specifically, the report states the following.

- Of 14 activities, 6 activities unreasonably delayed system analyses while 9 of 14 activities did not adequately support conclusions on Y2K compliance. Delayed analyses impaired critical management decisions, and improperly completed assessments provided false assurance that personnel either effectively ruled out or fully identified potential problems.

- Of 14 activities, 7 activities did not fully identify system interfaces, coordinate with interfacing system managers in a timely manner, or include system interfaces in their review process. Thorough, timely, and effective interface evaluations could help preclude errors between systems.

- Of 14 activities, 5 activities did not effectively schedule and prioritize renovations for systems assessed with Y2K problems. Properly prioritizing and scheduling renovations would promote efficiency, reduce workload, and help identify unneeded systems for potential retirement.

- Of 12 activities, 10 activities did not identify possible alternative actions or conduct the risk analyses necessary to preclude serious operational impact in the event that their systems failed. Effective contingency planning could preclude mission degradation and would enable the Air Force to maintain air and space superiority if a system crisis occurred.

The Air Force Communications and Information Center initiated actions to address the issues across the Air Force. Specifically, at the quarterly Air Force Y2K Working Group meetings, the Communications and Information Center personnel referenced the audit findings and gave top priority to those issues. Also, the Air Force Communications and Information Center informed all Air Force information technology personnel and program executive officers of the key Y2K areas requiring attention and action. Additionally, the Air Force Chief Information Officer sent a message to all major command vice commanders, center commanders, and program executive officers citing the audit results and emphasizing the need to strengthen Y2K oversight. Because of the multiple actions from senior Air Force leadership and the base-level reports of audit, the report made no recommendations.

Air Force Audit Agency Project No. 97066018, "Inventory Status for the Year 2000 Program," January 21, 1998. The report summarizes the audit results of 29 Air Force installation reports, listed in Appendix C in this report. The report states that Air Force organizations did not identify all reportable systems in the Y2K Air Force inventory database. Management identified nearly 2,100 systems before the audit and identified 5,809 additional systems throughout

the review. The inventory was incomplete because of problems associated with program guidance, senior management communication, and database organization.

Although DoD policy required that all systems be identified, Air Force program guidance did not sufficiently express that policy to prevent significant misinterpretations among reporting organizations. Additionally, the guidance did not specify a centralized process for identifying and analyzing off-the-shelf applications and information technology devices. Also, senior management at the command center and wing levels did not actively address the Y2K program with reporting organizations to ensure that they established full-time command/center/wing focal point positions with the authority to accomplish program goals, assigned unit representatives to interact with focal points, and coordinated effective working groups with active unit-level participation. Finally, the Air Force Y2K inventory database was not an effective and efficient tool to manage the Y2K data. Specifically, the database was not organized as an ongoing Air Force-wide project that required periodic updates and did not provide organizations with visibility over database contents or require unit-level reconciliations to increase data reliability.

The Air Force Communications and Information Center Director of Chief Information Officer Support published the updated Y2K guidance package, obtained support for the Y2K Program from the Secretary of the Air Force and the Air Force Chief of Staff, and implemented a new database to manage the inventory for computer systems in the Y2K program. The report considered the actions responsive to the issues raised and, therefore, made no recommendations.

Inspector General, Marine Corps

The Marine Corps conducted a review in May 1998 of its Y2K Program and identified issues related to areas of management, reporting, prioritization, interfaces, testing, contingency planning, assessment, and infrastructure. As a result of the review, in a memorandum dated July 31, 1998, the Commandant of the Marine Corps cited corrective actions and existing guidance to assist management in resolving Y2K issues. Also, briefings and a training shop were held to ensure that the Y2K coordinators from every major Marine Corps command worldwide were aware of the Y2K issues. The training workshop included discussions concerning the following:

- ongoing Y2K efforts;
- test plan development and contingency planning;
- Y2K system status;
- telecommunications, facilities, and miscellaneous items; and
- reporting requirements.

The overall emphasis of the briefings and training workshop was leadership and action at all levels of the command.

Appendix C. Air Force Audit Agency Installation Reports

The Air Force Audit Agency issued a management advisory letter titled, "Phase Status Validation for Year 2000 Program" (Phase Status Validation) and reports titled, "System Assessments for the Year 2000 Program" (System Assessments) and "Inventory Status for the Year 2000 Program" (Inventory Status) for various commands and installations as indicated in the following. The Air Force Audit Agency summarized the results of the installation reports and issued summary reports as shown in Appendix B.

Air Combat Command

Headquarters, Air Combat Command, Langley Air Force Base, Virginia,

- Phase Status Validation Project No. 98512022, June 29, 1998
- System Assessments Report No. 51298022, January 15, 1998
- Inventory Status Report No. 51297052, June 18, 1997

53d Wing, Eglin Air Force Base, Florida, Inventory Status Report No. 40397035, May 23, 1997

Air Education and Training Center

17th Training Wing, Goodfellow Air Force Base, Texas, Inventory Status Report No. 21397016, June 6, 1997

Air Force Center for Quality and Management Innovation

Air Force Center for Quality and Management Innovation, Inventory Status Randolph Air Force Base, Texas, Report No. 26497037, April 17, 1997

Air Force Materiel Command

Aeronautical Systems Center, Wright-Patterson Air Force Base, Ohio,

- Phase Status Validation Project No. 98445039, June 12, 1998
- Inventory Status Report No. 44597036, June 19, 1997

Air Force Materiel Command (cont'd)

Aerospace Maintenance and Regeneration Center, Davis-Monthan Air Force Base, Arizona, Inventory Status Report No. 20997016, May 9, 1997

Air Force Development Test Center, Eglin Air Force Base, Florida,

- Phase Status Validation Project No. 98403045, May 12, 1998
- Inventory Status Report No. 40397044, June 24, 1997

Air Force Flight Test Center, Edwards Air Force Base, California,

- Phase Status Validation Project No. 98402014, June 6, 1998
- System Assessments Report No. DD098001, April 1, 1998
- Inventory Status Report No. 40297019, June 18, 1997

Electronic Systems Center, Hanscom Air Force Base, Massachusetts,

- Phase Status Validation Project No. 98404035, May 8, 1998
- System Assessments Report No. 40498008, January 9, 1998
- Inventory Status Report No. 40497027, July 8, 1997

Human Systems Center, Brooks Air Force Base, Texas, Inventory Status Report No. 41097030, May 29, 1997

Ogden Air Logistics Center, Hill Air Force Base, Utah,

- Phase Status Validation Project No. 98405039, May 7, 1998
- System Assessments Report No. 40598016, November 17, 1997
- Inventory Status Report No. 40597056, May 15, 1997

Oklahoma City Air Logistics Center, Tinker Air Force Base, Oklahoma,

- Phase Status Validation Project No. 98440041, May 11, 1998
- System Assessments Report No. 44098007, December 23, 1997
- Inventory Status Report No. 44097028, June 27, 1997

Phillips Laboratory, Kirtland Air Force Base, New Mexico,

- System Assessments Report No. 23098011, March 17, 1998
- Inventory Status Report No. 23097014, June 9, 1997

Air Force Materiel Command (cont'd)

Sacramento Air Logistics Center, McClellan Air Force Base, California,

- Phase Status Validation Project No. 98415020, May 18, 1998
- System Assessments Report No. 41598006, January 30, 1998
- Inventory Status Report No. 41597020, June 17, 1997

San Antonio Air Logistics Center, Kelly Air Force Base, Texas,

- Phase Status Validation Project No. 98410020, May 26, 1998
- System Assessments Report No. 41098009, February 17, 1998
- Inventory Status Report No. 41097038, June 19, 1997

Space and Missile Systems Center, Los Angeles Air Force Base, California,

- Phase Status Validation Project No. 98412021, April 1998
- System Assessments Report No. 41298002, December 10, 1997
- Inventory Status Report No. 41297025, September 18, 1997

Space Systems Support Group, Peterson Air Force Base, Colorado,

- Phase Status Validation Project No. 98261020, April 20, 1998
- Inventory Status Report No. 26197043, August 26, 1997

Standard Systems Group, Gunter Annex, Maxwell Air Force Base, Alabama,

- Phase Status Validation Project No. 98516021, May 14, 1998
- System Assessments Report No. 51698001, October 9, 1997
- Inventory Status Report No. 51697008, July 18, 1997

Warner Robins Air Logistics Center, Robins Air Force Base, Georgia,

- Phase Status Validation Project No. 98425045, April 21, 1998
- System Assessments Report No. 42598019, January 17, 1998
- Inventory Status Report No. 42597052, June 18, 1997

Air Force Personnel Center

Headquarters, Air Force Personnel Center, Randolph Air Force Base, Texas,

- Phase Status Validation Project No. 98264024, April 15, 1998
- Inventory Status Report No. 26497035, May 6, 1997

Air Force Reserve Command

Headquarters, Air Force Reserve Command, Robins Air Force Base, Georgia, Inventory Status Report No. 42597049, June 13, 1997

Air Force Space Command

Headquarters, Air Force Space Command, Peterson Air Force Base, Colorado,

- Phase Status Validation Project No. 98261021, April 20, 1998
- Inventory Status Report No. 26197042, August 19, 1997

Air Force Special Operations Command

Headquarters, Air Force Special Operations Command, Hurlburt Field, Florida, Inventory Status Report No. 40397038, June 9, 1997

Air Intelligence Agency

Headquarters, Air Intelligence Agency, Kelly Air Force Base, Texas, Inventory Status Report No. 97058029, October 1, 1997

Air Mobility Command

Headquarters, Air Mobility Command, Scott Air Force Base, Illinois,

- Phase Status Validation Project No. 98265030, April 15, 1998
- Inventory Status Report No. 26597045, July 7, 1997

Pacific Air Forces

Headquarters, Pacific Air Forces, Hickam Air Force Base, Hawaii,

- Phase Status Validation Project No. 98220017, May 7, 1998
- System Assessments Report No. 22098001, November 24, 1997
- Inventory Status Report No. 22097015, June 26, 1997

United States Air Forces in Europe

Headquarters, U.S. Air Forces in Europe, Ramstein Air Base, Germany,

- Phase Status Validation Project No. 98522040, May 4, 1998
- Inventory Status Report No. 52297038, May 2, 1997

United States Strategic Command

Headquarters, U.S. Strategic Command, Offutt Air Force Base, Nebraska,

- Phase Status Validation Project No. 98520013, June 1998
- Inventory Status Report No. 52097017, May 19, 1997

United States Transportation Command

Headquarters, U.S. Transportation Command, Scott Air Force Base, Illinois,

- Phase Status Validation Project No. 98265029, April 22, 1998
- Inventory Status Report No. 26597046, July 8, 1997

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
- Deputy Under Secretary of Defense (Acquisition Reform)
- 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 Deputy-Y2K

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

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

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
Kathryn M.Truex
JoAnn Henderson
Scott S. Brittingham