

Audit



Report

SUMMARY OF DOD YEAR 2000
AUDIT AND INSPECTION REPORTS III

Report No. 99-247

September 3, 1999

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

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

Defense Hotline

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

Acronyms

AFMC	Air Force Materiel Command
CINC	Commander in Chief
COOP	Continuity of Operations Plan
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
GAO	General Accounting Office
GSA	General Services Administration
GPS	Global Positioning System
IG	Inspector General
MCAS	Marine Corps Air Station
MSC	Military Sealift Command
NATO	North Atlantic Treaty Organization
NAVSEA	Naval Sea Systems Command
NAWCWD	Naval Air Warfare Center, Weapons Division
OSD	Office of the Secretary of Defense
OSD (C ³ I)	Office of the Secretary of Defense (Command, Control, Communications, and Intelligence)
OMB	Office of Management and Budget
TOW	Tube Launched Optically Tracked Wire
USCENTCOM	United States Central Command
Y2K	Year 2000



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

September 3, 1999

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

SUBJECT: Summary of DoD Year 2000 Audit and Inspection Reports III
(Report No. 99-247)

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

Questions on the report should be directed to Ms. Maria R. Palladino at (703) 604-9007 (DSN 664-9007) (mpalladino@dodig.osd.mil) or Mr. James Hutchinson at (703) 604-9060 (DSN 664-9060) (jhutchinson@dodig.osd.mil). See Appendix B for the report distribution. The audit team members are listed inside the back cover.

A handwritten signature in black ink, reading "Robert J. Lieberman", is positioned above the typed name.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-247
(Project No. 8AS-0032.23)

September 3, 1999

Summary of DoD Year 2000 Audit and Inspection Reports III

Executive Summary

Introduction. This is the third summary report issued to discuss the DoD efforts to reduce year 2000 computing risks. This report summarizes 92 audit and inspection reports, briefings, and memorandums pertaining to DoD organizations, systems, and programs and their year 2000 conversion progress. The reports were issued from March through July 1999.

Results. If DoD sustains its focus on the year 2000 problem and avoids complacency, high confidence in its ability to avoid serious impairment to mission capability is justified. The number of compliant mission-critical systems has increased since the previous Inspector General, DoD, Report No. 99-115, "Summary of DoD Year 2000 Audit and Inspection Reports II," and extensive higher level testing is under way. Audit results indicate that additional work is needed to ensure that adequate testing is performed, testing results are sufficiently documented and analyzed, and contingency plans are viable. Host nation support and other international year 2000 issues also continue to present challenges for U.S. military forces.

Management Comments. We provided a draft of this report on August 19, 1999. 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	i
Introduction	
Background	1
Objective	2
Finding	
DoD Year 2000 Progress and Challenges	3
Appendixes	
A. Summaries of Year 2000 Audit and Inspection Reports and Memorandums	14
B. Report Distribution	73

Background

DoD Y2K Management Process. To achieve its year 2000 (Y2K) program goals and objectives, DoD adopted the five-phase management process as stipulated by the Office of Management and Budget (OMB). The first phase involves promotion of Y2K awareness. Successive phases involve system assessment, renovation, and testing of the Y2K fixes made. The last phase is concluded when a Y2K compliant system has been fully implemented. The DoD goal was to complete implementation of compliant mission-critical information systems by December 31, 1998. That goal was partly premised on the desire to operate systems for a full year in an effort to find "Y2K bugs" and to provide ample opportunity for further testing.

1999: The Year of Y2K Testing. DoD has completed Y2K renovation of almost all of its mission-critical information systems. As of June 30, 1999, DoD Components reported over 91 percent of critical DoD systems had been fixed, tested, and fielded. However, DoD Y2K efforts are far from finished. Although most systems have been individually tested and found to be Y2K compliant, DoD will devote the remainder of the year to ensuring, through operational readiness tests, that those individual systems will inter-operate properly on the arrival of Y2K. The ability of automated systems to process data correctly and exchange data successfully is critical to the accomplishment of virtually every military mission and support function. The operational readiness tests, or high-level tests, are especially challenging because of the number of systems involved, the risk of incompatible Y2K fixes, and an inflexible schedule.

DoD Guidance. In August 1998, the Deputy Secretary of Defense directed that Office of the Secretary of Defense (OSD) managers responsible for functional areas, such as logistics or personnel, conduct end-to-end tests of systems that support crucial functional processes. Because this level of testing was unprecedented, DoD issued Appendix I to the DoD Year 2000 Management Plan (DoD Y2K Management Plan) in June 1999. Appendix I provides guidance on planning, executing, and evaluating activities required to assess Y2K operational readiness from a functional perspective. It also describes relationships between functional end-to-end testing and other high-level testing activities performed by the Joint Staff and the Military Services. Joint Staff high-level testing will focus on those systems relied on by the Commanders in Chief during major theater warfare and the Military Services will perform high-level testing on systems related to weapon systems or other specific mission responsibilities.

Contingency Planning Requirements. On May 13, 1999, OMB requested that DoD and other selected Federal agencies develop an agency-level contingency plan. The contingency plan was to be written from a headquarters perspective and describe overall strategy and process for ensuring readiness of key programs and functions, rather than from an individual system perspective. Additionally, the contingency plan was to follow the guidance in the General Accounting Office (GAO) publication, "Year 2000 Computing Crisis: Business

Continuity and Contingency Planning,” August 1998. DoD submitted the agency-level contingency plan to OMB on June 15, 1999.

Although DoD has expended tremendous effort to find and fix potential Y2K problems, there is no guarantee that all Y2K problems have been discovered and remedied. Accordingly, the DoD Y2K Management Plan requires contingency plans be developed for each mission-critical system and the functions supported. These plans will help to ensure that system outages will be minimized and that the functions supported by the systems will continue despite any prolonged system disruptions. DoD components have developed literally thousands of system or operational contingency plans.

Objective

The objective of this report is to summarize Y2K issues identified in reports issued by the General Accounting Office; Inspector General, DoD; and Inspector General, Marine Corps; and the Army, Navy, and Air Force audit agencies from March 1999 through July 1999. Other audit and inspection organizations either did not issue written reports or did not furnish them for this summary. Appendix A provides a summary of the 92 reports, briefings, and memorandums involving DoD organizations.

DoD Year 2000 Progress and Challenges

If DoD continues its focus on the Y2K problem and avoids complacency, high confidence in the Department's ability to avoid serious impairment to mission capability is justified. The number of compliant mission-critical systems continues to rise, and extensive high-level testing is underway. However, additional work is needed to ensure that adequate Y2K testing is performed, test results are sufficiently documented and analyzed, and viable contingency plans are in place. In addition, host nation support and other international Y2K issues continue to present Y2K related risks to U.S. military forces. Other areas including the remaining noncompliant systems, military retiree pay, and military hospitals (identified by OMB as high-impact Federal programs) warrant continued management attention.

Progress Made in the Last Year

In the latest quarterly report to OMB, DoD showed steady progress in the number of compliant mission-critical systems, as well as in the percentage of mission-critical systems that have completed the renovation, validation, and implementation phases.

The status of DoD mission-critical systems was briefed to the Secretary of Defense on July 21, 1999, and the reported number of completed mission-critical systems increased to 1,940. That brought the percentage of completed mission-critical systems to 92 percent. Only 167 mission-critical systems remained to be completed before December 31, 1999. Examples of the remaining noncompliant systems included:

- Tooele Chemical Demilitarization Facility Control System,
- Standard Installation/Division Personnel System-3,
- Navy Military Personnel Distribution System,
- Advanced Combat Direction System Block 0,
- Digital Terrain Analysis Mapping System,
- Contingency Theater Automated Planning System,
- F-117A Mission Planning System,
- Standard Finance System,
- Standard Army Financial Inventory Accounting and Reporting System,
- Future Years Defense Program,

-
- Point of Sales – Modernization,
 - Signal Intelligence Processors, and
 - Defense Switched Network

Results of DoD Audits and Inspections

This report summarizes 92 audit and inspection reports, briefings, and memorandums issued from March through July 1999. The reports continue to identify shortfalls within the DoD Components, but the shortfalls have decreased for several risk areas when compared to the previous Inspector General, DoD, Summary Report. A precise conclusion cannot be drawn from the comparison because the objectives and scope of the audits may have varied.

Examples of Significant Progress

Previous summary reports identified several risk areas that continued to pose significant challenges to DoD, including supplier outreach and mainframe computer compliance. Significant progress has been made in these 2 areas.

Supplier Outreach. The Defense Logistics Agency (DLA) and the Deputy Under Secretary of Defense (Logistics) identified over 5,100 critical suppliers and grouped them based on DoD reliance on their capabilities. DoD Y2K compliance assessments are being performed on those suppliers of which DoD is extremely reliant. Over 2,200 suppliers were categorized as either moderately or highly critical and required an on-site visit to complete the Y2K compliance assessment. A DoD assessment is underway based on evaluations completed in April 1999. Follow-on prime vendor testing was planned through July 1999. In addition, the DLA Senior Procurement Executive sent a letter to the critical suppliers addressing the importance of the readiness of automated systems and stressed the importance of government and industry working together to evaluate the supply chain of products and services critical to the DoD mission.

Mainframe Computer Compliance. Functional applications that run on mainframe computers operate in a logical partition called a domain. The Defense Information Systems Agency (DISA) owns and operates most DoD mainframes and provides computer processing services to other DoD Components, that own and maintain the functional applications. All primary elements of a domain (the application, the hardware, and the executive software) have to be considered before the entire system is deemed to be Y2K compliant. As of June 1999, 38 percent of DISA mainframe domains processing mission-critical applications were certified Y2K compliant. As of July 30, 1999, the percentage of mainframe domains that had been completed had increased to 95 percent.

Y2K Testing and Contingency Planning Challenges

Although DoD continues to make progress in solving its Y2K problem, the complexity and interrelationships of DoD automated systems continue to provide management significant challenges in several areas. Foremost are determining and conducting appropriate levels of testing and ensuring the viability of contingency plans.

Testing. The DoD Y2K Management Plan requires that all mission-critical automated systems undergo two different levels of testing. At the first level, individual systems are validated, or tested, to ensure that the system is Y2K compliant and performs as intended. Commonly referred to as certification testing, the first-level test should be the most rigorous and thorough and provides DoD the primary assurance that the system will operate correctly in the year 2000. The second-level testing has a higher focus in that its primary intent is to ensure that a related group of systems inter-operate correctly. Higher level testing helps to ensure that strings of systems involved in the critical path of military operations and systems used in essential support functions are Y2K compliant. High-level testing is not as vigorous as certification testing, and could be viewed as the Y2K graduation exercise. Defining the appropriate scope and vigor of testing at both levels continues to challenge DoD managers.

Certification Testing. Previous Inspector General, DoD, reports have cautioned senior DoD managers about the risks involved with system self-certification. The certifications of hundreds of DoD mission-critical systems were originally based on self-certification instead of independent testing. DoD has come to recognize that self-certification is inherently more risky than independent testing. Accordingly, senior DoD managers have emphasized that all self-certified systems should undergo independent validation of the testing or testing results. The use of automated Y2K tools called code scanners has identified hundreds of Y2K errors in systems previously self-certified Y2K compliant. Also, the use of time machine testing has identified additional Y2K errors not detected during certification testing. Time machine testing is the testing of systems in a dedicated operational environment in which the computer's internal date and time is set to the time period being tested. Initial certification testing was often performed in environments in which one or more of the system date and time clocks were simulated. For instance, certification testing of application programs may have been performed through simulated date changes instead of using date changes generated by the computer.

The results of code scanning and time machines testing have vividly demonstrated flaws in the scope and vigor of initial Y2K certification testing. Although DoD managers have initiated efforts to more stringently examine self-certified systems, the completion of that effort prior to Y2K is an ambitious goal. As of June 25, 1999, almost 200 systems had to complete more intensive testing. Because the re-examination of certified systems is a relatively new DoD thrust, the resources and time required may detract from accomplishing other Y2K activities and may subject the scheduled completion of those activities to substantial risk.

Further, the weaknesses demonstrated with initial certification testing, the testing process relied on by DoD officials for primary Y2K assurance, compounds the risks associated with the known limitations of higher level testing.

High-Level Testing. To meet Congressional requirements and to provide assurance that DoD mission accomplishment would not be adversely impacted by Y2K errors, DoD testing focus is directed at the various "system of systems" vital to the accomplishment of military missions and critical to supporting functions. DoD high-level testing is being accomplished through three primary mechanisms:

- Commander in Chief (CINC) thinline testing is the testing of systems critical to the areas of responsibility of each CINC of the Unified Commands. Testing occurs during operational evaluations, which are conducted to evaluate the operational effectiveness of a unified command.
- Integration testing is the testing of systems critical to mission performance by each Military Service. Testing occurs during military exercises, and is designed to assess the potential Y2K impact on systems related to a particular weapon system or to specific Military Service mission responsibility.
- Functional end-to-end testing is the testing of functional support systems vital to the accomplishment of critical military missions. End-to-end test planning and oversight is the responsibility of OSD principal staff assistants in charge of warfighter functional support areas, such as communications or logistics.

If performed properly, high-level testing augments system certification testing in several ways. It is supposed to present new test cases to be processed by critical applications in each string of systems. It should also test critical interface paths between each system in the string through actual data interchanges. However, as in any type of testing, responsible managers are continually challenged to find the appropriate balance between sufficient testing and available testing resources. With Y2K testing, the most critical resource is time. Y2K is less than 6 months away. Preliminary results of several ongoing audits and other high-level testing reviews indicate that DoD managers may have sacrificed sufficient testing rigor and scope to meet an inflexible schedule.

Preliminary high-level test results. Very few Y2K failures have been discovered during the various high-level tests. On the surface, such successful test results are encouraging, since they may indicate a particularly efficient remediation effort. However, finding relatively few Y2K errors also raises the obvious question of whether the high-level testing is sufficiently rigorous. That question becomes even more of a concern for DoD managers in light of the number of numerous additional errors found through the use of code scanning or time machine testing on previously certified systems.

Limitations. The DoD high-level tests are being conducted with several acknowledged limitations:

- Minimum applications, interfaces, and dates are being tested.
- The clocks of some mission-critical DoD systems included in the high-level test strings cannot be set forward without substantial risk of total system failure.
- Simulated operational environments and test systems are being used instead of operational systems and realistic operational environments.
- Some strings of systems being tested are incomplete because systems are not yet certified as Y2K compliant or are not participating in the high-level test.

We are not aware of any high-level test that has been or is being conducted with all of the described limitations. Nor do we believe that one or more of these limitations are sufficiently serious to offset the potential benefits of high-level testing. However, as illustrated in the following topical discussion, each testing limitation has attendant risks. Master test plans for some high-level tests describe testing limitations, but do not describe the associated risks. Unless testing limitations and associated risks are collectively assessed, it is not clear how senior managers can effectively evaluate the planned testing methodology or meaningfully interpret test results.

Testing for Interoperability. The primary objective of high-level testing is to provide additional assurance that related systems interoperate correctly. Effective interface testing is key to ensuring DoD mission-critical systems can connect with other systems and will send and receive only Y2K compliant data.

DoD requires, with limited exceptions, that all system interfaces be tested with operational data during certification testing. Figure 1 illustrates a system with multiple internal and external interfaces.

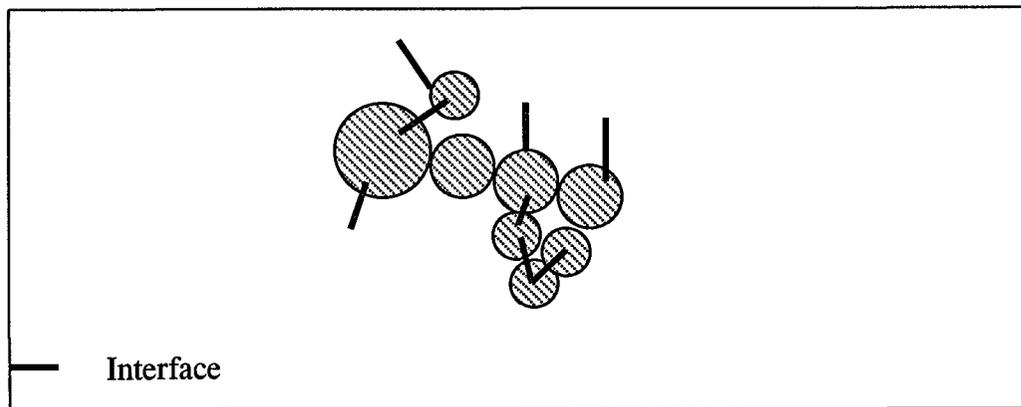


Figure 1. Example of Internal and External Interfaces

During previous audits, we found that the certification testing of some mission-critical systems did not include actual interface testing. Managers had deferred actual external interface testing to the high-level testing activities. However, the inclusion of systems in higher level testing is not an acceptable substitute for rigorous certification testing because high-level interface testing includes only the necessary system interfaces to meet the specific requirements of the string being tested. Accordingly, many of a system's external interface partners are excluded during high-level interface testing. Figure 2 illustrates how some external interfaces may be excluded during high-level interface testing.

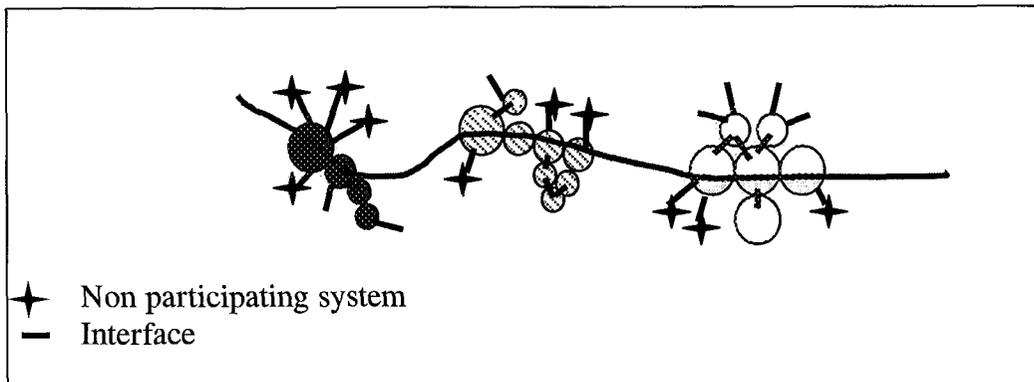


Figure 2. External System Interfaces May Not be Included in High-Level Interface Testing

If detailed external interface testing was not performed during certification tests of each system included in the string, the risk is unacceptably high that some system interfaces do not perform accurately. Accordingly, senior DoD managers would have little assurance that invalid data will not be introduced and propagated throughout the high-level string of systems.

Contingency Plans. Despite the best efforts of DoD to meet the Y2K challenge, there is no certainty that automated systems will not be impacted by Y2K failure. Failure in a single system could impact several other systems. Accordingly, DoD requires that contingency plans be developed and tested to ensure that organizations can continue to meet their mission, regardless of the availability of related automated systems. Two types of contingency plans are required:

- system contingency plans that detail procedures necessary to restore a system in the face of all Y2K disruption, and
- operational contingency plans that detail procedures by which the mission or function supported will be continued during any prolonged disruption.

The DoD Y2K Management Plan provides contingency planning guidance and requirements. For all mission-critical systems, system contingency plans were to be completed by December 30, 1998, and operational contingency plans were to be completed by March 31, 1999. To assure viability, both types of contingency plans were to be tested by June 30, 1999. As the end of the year

approaches, the need for contingency plans becomes more important because the risk of late completion of systems and testing grows.

Our previous summary report discussed 23 audit and inspection reports that identified shortfalls in contingency planning. This report summarizes another 45 reports that describe less than adequate contingency planning efforts. Further, 19 ongoing audits or inspections have tentatively identified contingency planning issues associated with additional DoD mission-critical systems or functional organizations.

We recognize that DoD organizations are working to remedy known Y2K problems and that the necessary resources to focus on other aspects of Y2K, such as contingency planning, may be difficult to identify. Nonetheless, the sheer number of contingency planning problems identified is a good indicator that some DoD managers may not have appropriately emphasized the importance of thorough and effective contingency plans. To help provide that emphasis, we will continue to include reviews of contingency plans and their viability as a part of our ongoing Y2K audit coverage.

DoD Participation in International Outreach Efforts

DoD focused its Y2K international outreach efforts in three primary areas: host nation support, NATO (North Atlantic Treaty Organization), and Russia. Both the Under Secretary of Defense (Policy) and the Director, OSD Y2K Outreach are involved in these efforts.

Host Nation Support Remains a Y2K Challenge. The potential Y2K impact on U.S. military forces based in foreign countries is still far from defined. DoD often depends on host nations to provide communications and infrastructure support to DoD facilities and forces based in the host country. Generally, the probability of widespread and serious Y2K failures in foreign countries is perceived to be much higher than in the United States. Unfortunately, little reliable information about the Y2K status of host nations is available. For example, Inspector General, DoD, Report No. 99-163, "Year 2000 Issues within the U.S. Pacific Command's Area of Responsibility Host Nation Support to U.S. Forces Korea," May 17, 1999, stated that the U.S. Forces Korea had not obtained interface agreements or formal assurances of Y2K compliance from the Republic of Korea civil and military (government) organizations and commercially operated companies providing armistice and wartime host nation support. Following initial audit briefing results, U.S. Forces Korea took aggressive and effective action to begin coordination efforts with the Republic of Korea to discuss mutual Y2K efforts and issues.

Joint Staff Efforts. The Joint Staff has initiated efforts to better define the likelihood of host nation Y2K failure and its potential impact on military facilities in foreign countries. These initial efforts highlight the fact that little information is readily available. A Joint Staff briefing to the Secretary of Defense on July 21, 1999, provided an assessment of the Y2K compliance of host nation services provided to DoD outside the Continental United States installations, as well as an evaluation of non-DoD installations vital to the

execution of Operations Plans. Areas of Host Nation Support discussed included communications, energy, finance, safety, sewage, transportation, and water. The following are host nation support issues that need to be addressed:

- 22 of 30 countries and 78 of 95 installations are still unknown,
- 20 of 30 countries and 60 of 95 installations have low-confidence services, and
- 19 of 30 countries have mismatches in available information, as well as the availability and comparison of other assessments.

The Joint Staff briefed that the OSD is leading the effort in conjunction with State Department and Regional Assessment Teams. In addition, the Joint Staff and CINCs are prioritizing countries and installations and assessing host nation support Y2K risks on Operations Plans execution. The Services are also refining Continuity of Operations Plans to address host nation support issues.

Under Secretary of Defense (Policy) Efforts. The Under Secretary of Defense (Policy), in his briefing to the Secretary of Defense, stated that the goal regarding host nation support issues is to provide geographic CINCs with information regarding Y2K vulnerabilities of critical infrastructures at the national level and in key regions to support operations and contingency planning for the transition period. Specific host nation support issues identified include:

- facilities that are vital to CINC Operations are not under U.S. control,
- Y2K awareness varies widely between and within countries, and
- cultural factors impede speed and cooperation of information collection efforts.

The approach to address host nation support issues includes conducting targeted regional infrastructure assessments and co-chairing an international working group with the Department of State. In addition, in the next 6 months, DoD will work through the CINC Y2K offices to normalize and update the Joint Staff host nation assessment baseline, deploy regional assessment teams to the CINCs, and support CINC Table Top exercises for Y2K contingency plan validation.

Additionally, preliminary Y2K assessments from different DoD organizations are often in conflict. Accordingly, DoD plans to establish regional assessment teams to visit host nations. Until the Y2K status of host nations is better defined and understood, DoD managers cannot effectively formulate appropriate risk reduction plans.

NATO. DoD has established two goals for outreach efforts with NATO. The first is to ensure the continuity of the Stabilization Force and the Kosovo Peacekeeping Force operations over the Y2K transition. The second is to obtain insight into the Y2K status of member nation systems that will affect other

coalition operations. DoD's approach to reach these goals includes participating in the monthly NATO Integrated Process Team meetings and assisting the Supreme Headquarters Allied Powers, Europe, Y2K Program Management Office.

In the next 6 months, DoD will continue to support the NATO Integrated Process Team and Program Management Office. However, several issues are a concern for DoD including getting a late start on operational issues, poor participation by member nations in the NATO Integrated Process Team, failure to develop an integrated approach among NATO entities, and slow progress on Continuity of Operations plans.

Russia. In its coordinated approach for international outreach to Russia, DoD goals include to ensure the stability of nuclear arsenals and to promote Military-to-Military cooperation. The approach thus far has been to leverage the existing programs and to coordinate the DoD integrated program through OSD Y2K outreach. The program consists of five pillars:

- Technology Management – share Y2K management practices, expertise, and lessons learned;
- Special Communication Links – ensure secure communications between U.S. and Russian political and military leaders during the Y2K transition;
- Nuclear Stockpile Security – ensure control, security, and accountability of Russia's nuclear materials, stockpiles, and weapons labs, during the Y2K transition;
- Center for Y2K Strategic Stability – host exchange of U.S. and Russian missile launch information at special center in Colorado Springs to reduce the risk of misunderstandings from Y2K related malfunctions in early warning systems; and
- Nuclear Forces Command and Control – exchange Y2K management information, status, and experiences specific to nuclear systems.

Actions planned for the next 6 months include sending letters to Russian Ministries of Defense and Foreign Affairs suggesting reengagement on Y2K activities, holding a coordinated meeting in August, and working all five pillars independently under a coordinated umbrella through March 2000. An August 1, 1999, reengagement was essential for secure communications given the required lead time for procurement, installation, and testing. DoD is uncertain about the timing and extent of Russian willingness to reengage on the remaining program.

Areas that Warrant Continued Management Attention

Late Completion of Systems. DoD has made significant progress during the past year in assessing, fixing, and implementing Y2K compliant systems.

Further, DoD forecasts that all mission-critical systems will be fully implemented by the end of 1999. However, DoD did not meet its goal of completing all mission-critical systems by December 31, 1998. In the monthly report to OMB, June 1999, DoD reported that 25 mission-critical systems are scheduled to be completed after September 1999. Some systems are not scheduled to be completed until December 1999.

High-Impact Federal Programs. In March 1999, the OMB identified several areas of potential high-impact on the American public if serious Y2K failures should occur. Two high-impact areas, military retirement and military hospitals, were assigned to DoD as the lead agency. As the assigned lead, DoD is responsible for assuring that Y2K problems have been addressed, jointly determining with any partners that the Federal program will work, and publicly demonstrating that it will.

The Defense Finance and Accounting Service has the lead for military retiree pay and the Assistant Secretary of Defense (Health Affairs) has the lead for military hospitals. Recent audits have shown that both organizations have relatively strong Y2K programs; the Y2K programs of both organizations have experienced Y2K problems, such as executing Y2K end-to-end tests on schedule. Although the Y2K problems are relatively minor, even minor Y2K failures in systems related to the designated high-impact areas could seriously undermine public confidence. DoD may need to make special efforts to assure beneficiaries that service will not be disrupted.

Y2K Configuration Management Policy Implementation. Software is routinely upgraded to provide increased functionality, to meet legal requirements, or to ensure interoperability with other systems. However, the fielding of new or upgraded software into an existing configuration of systems that have been tested, certified as Y2K compliant, and function properly in an operational environment, creates the risk that the new software will not function properly and may cause systems that were Y2K compliant to no longer be Y2K compliant.

The DoD Y2K Management Plan recommends that rigorous procedures be developed to ensure that system modifications do not invalidate the functional and operational testing that has been completed. Accordingly, DoD developed, and issued on August 20, 1999, a centralized DoD policy to ensure effective configuration management of mission critical system architectures after completion of Y2K testing. That policy, effective from September 1, 1999, through March 15, 2000, should balance the need to continually update and enhance software with the need to prudently manage risks associated with introducing changes into Y2K compliant system architectures. However, the development of that policy was more complex than anticipated and the associated coordination discussions were often contentious. The Inspector General, DoD, was directed to monitor and report to the DoD Chief Information Officer on the efficiency and effectiveness of the configuration management process established in the policy.

Conclusion

Audit results are consistent with management reporting that indicates that DoD continues to make good progress in addressing Y2K issues. However, audit results also indicate that considerably more work is needed in several areas. Specifically, DoD needs to ensure that adequate testing is performed and contingency plans are tested for viability to reduce Y2K related risks. In addition, host nation support continues to present Y2K related risks to U.S. military forces. Other areas that warrant management attention include the remaining noncompliant systems, military retiree pay and military hospitals (which were identified by OMB as high-impact Federal programs), and the development of Y2K configuration management policy.

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

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

General Accounting Office

Report No. T-AIMD-99-187, "Time Issues Affecting the Global Positioning System," May 12, 1999. GAO testified that, according to the Air Force Materiel Command (AFMC), the executive agent for the DoD in acquiring Global Positioning System (GPS) satellites, all GPS satellites are Y2K compliant. The space component of the GPS includes satellite support systems. These systems are responsible for maintenance and proper functioning of the satellites. The support systems consist of ground and user components. The ground support systems are interconnected through networks and have information systems and equipment that must be renovated for Y2K compliance. According to the AFMC, the ground support systems are now Y2K compliant. Contingency plans are also in place for these systems. The user support systems consist of receivers, processors, and antennas that allow land, sea, or airborne operators to receive the GPS satellite broadcast and compute their precise position, velocity, and time. According to the AFMC, many newer GPS receivers have been tested and have demonstrated that they are Y2K compliant. For organizations and individual users that have older GPS receivers, it is vital that they make an effort to determine whether the networks they operate rely on GPS equipment as a time source and the potential GPS-related risks.

Report No. AIMD-99-154, "Year 2000 Computing Crisis: Costs and Planned Use of Emergency Funds," April 28, 1999. The report stated that according to the February 1999 quarterly status reports to OMB, the total estimated Y2K cost for the 24 major federal agencies is about \$7.5 billion. This estimate has more than tripled from the \$2.3 billion estimate in February 1997. The agencies reported to us that less than half of the \$7.5 billion in Y2K costs had been incurred prior to fiscal year 1999. However, these reported costs were generally estimates and not actual costs. Of the 24 major agencies, only 7 reported that they separately tracked actual costs of Y2K activities and 5 reported that they tracked some actual costs and estimated other costs.

The lack of tracking of Y2K costs was also reflected in the reported obligations for the first quarter of fiscal year 1999. Obligations of \$68.4 million for Y2K costs were reported by 24 organizations, including 2 organizations that reported only obligations of emergency funds. However, eight organizations did not

know what their obligations of appropriated and emergency funds were for the quarter and the remaining nine organizations, including five major agencies, did not provide obligation information.

The estimated Y2K costs reported by the 24 major agencies for fiscal year 1999 have increased during the last year from about \$1.1 billion in February 1998 to \$2.8 billion in February 1999. The civil agencies plan to use the emergency funds for a variety of activities including renovation, validation, and implementation of systems; replacement of personal computers and network hardware and software; outreach; and independent verification and validation. DoD plans to use emergency funds for testing, operational evaluations, and contingency planning. According to their justification submissions, organizations requested emergency funds because they identified new requirements such as outreach activities and decisions to replace personal computers and networks; had increased costs of ongoing Y2K activities; and/or regular appropriations were not available for planned Y2K activities.

Report No. T-AIMD-99-149, "Year 2000 Computing Crisis: Readiness Improving But Much Work Remains to Ensure Delivery of Critical Services," April 19, 1999. GAO testified that the public faces a risk that critical services provided by the government and the private sector could be severely disrupted by the Y2K computing problem. Financial transactions could be delayed, flights grounded, power lost, and national defense affected. Moreover, America's infrastructures are a complex array of public and private enterprises with many interdependencies at all levels. These many interdependencies among governments and within key economic sectors could cause a single failure to have adverse repercussions in other sectors. Key sectors that could be seriously affected if their systems are not Y2K compliant include information and telecommunications; banking and finance; health, safety, and emergency services; transportation; power and water; and manufacturing and small business.

The federal government's reports as of April 1999, showed improvement in addressing the Y2K problem. While much work remains, the federal government has significantly increased the percentage of mission-critical systems that are reported to be Y2K compliant. In 1999, 92 percent of mission-critical systems were reported to be compliant as of March 1999.

While improvement has been shown, much work remains at the national, federal, state, and local level to ensure that major service disruptions do not occur. Specifically, remediation must be completed, end-to-end testing performed, and business continuity and contingency plans developed. To meet this challenge, strong leadership and partnerships must be maintained to ensure that government programs meet the needs of the public at the turn of the century.

Report No. AIMD-99-144, "Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions," April 14, 1999. The GAO testified that progress had been made on the Y2K problem. However, many key tasks remain that need to be completed to ensure the continuity of critical services. Specifically, complete and thorough testing is

essential to provide reasonable assurance that new or modified systems process dates correctly and will not jeopardize an agency's ability to perform core business operations. DoD was cited for showing evidence of progress, but OMB still has concerns. Not all of the systems reported as compliant have completed an independent verification process. In some cases, systems that had completed an independent verification and validation process were found to have serious problems. Also, many of the mission-critical systems that were not implemented by the March target date support critical business processes, and some are not scheduled to be Y2K compliant for several months. In February 1999, the GAO testified that many state systems would not be compliant until the last half of 1999. The GAO concluded that business continuity and contingency planning was even more important in ensuring the continuity of operations.

The report stated that in January 1999, GAO testified that OMB should consider setting target dates for developing end-to-end test plans, establishing test schedules, and completing the tests for the government's most critical functions. The report also stated that in January 1999, GAO testified that OMB could consider setting a target date, such as April 30, 1999, for the completion for business continuity and contingency plans, and require agencies to report on their progress against that milestone, so that the OMB would have more complete information on this critical issue. GAO also suggested that OMB consider requiring agencies to test their business continuity strategy and set a target date, such as September 30, 1999, for the completion of this validation.

Report No. T-AIMD-99-143, "Year 2000 Computing Crisis: Additional Work Remains to Ensure Delivery of Critical Services," April 13, 1999. GAO testified that the federal government has significantly increased the percentage of mission-critical systems that are reported to be Y2K compliant. However, 11 agencies did not meet OMB's deadline for all of their mission-critical systems. Some of the systems that were not yet compliant support vital government functions. As GAO testified last month, several of these systems provide critical functions, ranging from communications to radar processing to weather surveillance.

Not all systems have undergone independent verification and validation. In some cases, independent verification and validation of compliant systems have found serious problems. Although individual system compliance, is important it does not necessarily ensure that a business function will continue to operate through the change of the century. End-to-end testing and business continuity and contingency planning are vital to ensuring that this goal is met. Further, OMB has recently taken action on GAO's April 1998 recommendation to set government-wide priorities and has identified the government's high-impact programs.

OMB's March 1999 memorandum identifies several high-impact state-administered programs that both the federal government and the states have huge vested interests, both financial and social. There is need for the lead federal agency to work together with the states to ensure that federal human services programs can continue through the Year 2000.

Report No. AIMD-99-101, "Defense Has Made Progress, But Additional Management Controls Are Needed," March 2, 1999. The GAO testified to Congress that DoD had taken steps to strengthen management of its Y2K program by providing the controls and guidance needed to fix and test systems. In addition, DoD had appropriately shifted its focus to core business readiness and operational risks. Specifically, DoD performed end-to-end tests, executed simulated Y2K operational exercises, and conducted system integration tests. However, DoD faced two significant challenges and a fast approaching deadline. First, DoD must catch up and complete remediation and testing of mission-critical systems. Second, it must have a reasonable level of assurance that key processes (functional areas) will continue to work on a day-to-day basis and key operational missions necessary for national defense can be successfully accomplished.

Specifically, the Department needed to determine the:

- status of each supporting information system critical to that process including its schedule for remediation and testing,
- source and Y2K status of any suppliers or vendors critical to that process,
- outside dependencies (such as electrical power) that affect readiness,
- interfaces with other processes and outside organizations,
- scope and schedule of end-to-end testing for the process, and
- scope and schedule for business continuity planning for that process.

For any of these elements that were behind schedule, DoD needed to know what steps will be taken to get back on schedule and what steps will be taken to minimize the risks associated with their delay. This information was critical in identifying those areas where DoD faced the greatest risk of failure and critical to providing the necessary data for preparing overall business continuity plans.

Office of the Inspector General, DoD¹

Report No. 99-227, "Year 2000 Posture of Mid-Tier Computer Systems Processing Defense Finance and Accounting Service Data," July 29, 1999. The report stated that Defense Finance and Accounting Service (DFAS) managers were aware of and actively involved in achieving compliance with the

¹ The full text of Inspector General, DoD, reports is available on the Internet at <http://www.dodig.osd.mil> and summaries of Y2K audit activity are accessible at <http://www.ignet.gov>.

DoD Y2K Management Plan. However, in March 1999, DFAS was not fully assured that mid-tier computer systems would be Y2K compliant because:

- the inventory of mid-tier computer systems was not fully reconciled and updated,
- test plans were not developed and the results of testing were not documented for mid-tier computer systems,
- managers and users of systems that interface with DFAS mid-tier computer systems needed to be more involved in contingency planning, and
- five systems were not certified as being tested on Y2K compliant mid-tier computers.

As a result, DFAS needed additional effort to mitigate risk that its mid-tier computer systems would not successfully process Y2K-related data. The Inspector General, DoD, recommended that the Director, Defense Finance and Accounting Service, periodically reconcile and update its inventory of mid-tier computer systems; develop Y2K test plans for the systems, including plans for testing interfaces; ensure that contingency planning involved system users or managers that had interfaces with the DFAS systems; and certify systems that were tested on Y2K compliant mid-tier computers.

DFAS concurred with the recommendation to reconcile and update the inventory of mid-tier computer systems, and stated that corrective actions were in progress as of June 4, 1999. DFAS partially concurred with updating test plans, however, it stated that it was too late to standardize testing procedures because the systems were already tested and certified. Also, DFAS agreed, as of June 4, 1999, to make a special effort toward emphasizing the importance of coordinating and providing information to its interfacing partners. Finally, DFAS concurred with certifying systems as being tested on Y2K compliant mid-tier computers. It stated that each of the 17 reviewed DFAS systems were certified as Y2K compliant, and indicated that all of the systems were implemented.

The DFAS comments were responsive and no further management comments were required.

Report No. 99-215, “Year 2000 Computing Issues: Defense Logistics Agency - Standard Automated Materiel Management System,” July 16, 1999. The report stated that the DLA and its three subordinate supply centers had taken action to ensure that the Standard Automated Materiel Management System, which provides support to the DLA for the management of consumable items, would be Y2K compliant. Specifically, DLA:

- implemented Y2K contract clauses,
- allocated necessary funds,

-
- implemented an information assurance program,
 - established management oversight and reporting,
 - prioritized and inventoried mission-critical systems and infrastructure,
 - developed contingency and test plans, and
 - performed Y2K testing.

However, DLA did not fully comply with the requirements of the DoD Y2K Management Plan. DLA failed to comply because it did not fully document interfaces; did not document all test results; did not meet the Y2K certification milestone of December 31, 1998; and did not test the Standard Automated Materiel Management System in a Y2K compliant domain. Although DLA did not fully comply, it subjected the Standard Automated Materiel Management System to intensive testing before certification. Additional testing and logistics end-to-end testing was to provide further assurance that the DLA core supply mission performed by the Standard Automated Materiel Management System would be Y2K compliant.

The Inspector General, DoD, recommended that the Director, Defense Logistics Agency, review the Standard Automated Materiel Management System interfaces to ensure that the critical thread interfaces were identified and tested during the logistics functional end-to-end testing that was scheduled from April through June 1999.

DLA concurred with the recommendation, stating that a function of the end-to-end testing plan was to ensure that all critical thread interfaces were identified and included in the test.

Report No. 99-213, “Year 2000 Compliance of Selected Headquarters Standard Systems Group Systems,” July 14, 1999. The report stated that the Headquarters Standard Systems Group Systems management implemented a certification process that verified and certified its systems. The Headquarters Standard Systems Group program managers tested the Logistics Module and the Contingency Operations Mobility Planning Execution System to ensure that system and interface interoperability were Y2K compliant.

The Headquarters Standard Systems Group Y2K policy requires managers to obtain independent verification of system testing and to prepare system contingency plans. However, the Logistics Module and the Contingency Operations Mobility Planning Execution System contingency plans were not effective in identifying actions to preserve and protect the system and data before, during, and after a Y2K related failure. Consequently, the Logistics Module and Contingency Operations Mobility Planning Execution System contingency plans do not provide the user with all necessary procedures that would expedite restoration of the systems and continuation of essential functions, should the system fail.

The Inspector General, DoD, recommended that the Director, Headquarters Standard Systems Group:

- prepare contingency plans for the Logistics Module and Contingency Operations Mobility Planning Execution System in accordance with the DoD Y2K Management Plan,
- validate that the contingency plans are executable, and
- distribute the contingency plans to system users.

The Air Force planned actions that are in progress to meet the intentions of the recommendations and action should be completed by August 31, 1999.

Report No. 99-207, “Year 2000 Compliance of the Theater Deployable Communications System,” July 7, 1999. The report stated that the Electronic Systems Center Program, Director for Defense Information Infrastructure, certified the Theater Deployable Communications system as Y2K compliant on December 31, 1998. The system program manager followed the Electronic Systems Center certification process documented in the Y2K Corrective Action Plan. The plan requires comprehensive verification of system testing before certification. The certification of the Theater Deployable Communications system and deployment of contingency plans minimized the risk of system failure associated with Y2K processing.

Report No. 99-204, “Year 2000 Status of the Combat Control System Mark 2 Block 1 A/B,” July 9, 1999. The report stated that the Naval Sea Systems Command (NAVSEA) certified the Combat Control System Mark 2 Block 1 A/B as Y2K compliant on October 31, 1997, using criteria that were subsequently superceded. The NAVSEA did not have documentation to support that the following steps took place before system certification:

- confirming that the system was Y2K compliant through date testing,
- determining that the system software and hardware were Y2K compliant, and
- testing and certifying all system interfaces as Y2K compliant.

In addition, the NAVSEA checklist differed substantially from the DoD Y2K Management Plan checklist and did not comply with the Navy Y2K Action Plan. As a result, system level testing was incomplete when the Combat Controlled Systems Mark 2 Block 1 A/B was reported as compliant in the DoD Y2K database. However, additional testing was performed after certification, and because the testing appeared to be adequate, the Y2K compliance status of the Combat Controlled Systems Mark 2 Block 1 A/B was no longer the issue. Although the additional testing was sufficient to alleviate concerns about this particular system, the methodology used for its certification raised concerns that 127 other NAVSEA systems certified as of September 1998 might also have been prematurely and inappropriately certified as Y2K compliant.

It was recommended that the Chief Information Officer, Navy, review the adequacy of system level testing as a risk mitigation step for the other NAVSEA mission-critical systems that were certified as of September 1998.

The Chief Information Officer, Navy, nonconcurrent with the draft recommendation, which was to determine if recertification was necessary. He stated that recertification was not necessary for the other mission-critical systems certified as of September 1998 because of the extensive testing performed by the NAVSEA.

The Inspector General, DoD, considered the comments of the Chief Information Officer, Navy, to be nonresponsive. The issue raised in this report was whether the system level testing for all NAVSEA systems, other than the Combat Controlled Systems Mark 2 Block 1 A/B, was adequate, whether performed before or after certification. To focus attention on that issue, and not on the formalities of certification, the recommendation was reworded. As a result, the Inspector General, DoD, maintained that an additional risk existed if the individual components were not tested individually in conjunction with the application testing. Also, the checklist used to certify the system contained substantive differences from the DoD Management Plan Y2K Compliance Checklist, which covers more Y2K compliance issues than the NAVSEA checklist. Accordingly, the Navy needed to determine whether adequate system certification testing occurred for the other 127 NAVSEA mission-critical systems, regardless of when it occurred. The Navy was asked to reconsider its position on the revised recommendations. The Navy has not yet commented and action is still ongoing.

Report No. 99-202, "Year 2000 Compliance of Selected Mission Critical Command, Control, and Communications Systems Managed by the Defense Information Systems Agency," July 2, 1999. The report stated that the Defense Information Systems Agency had made substantial progress to ensure that the mission-critical systems were Y2K compliant in accordance with the DoD Y2K Management Plan. As of May 17, 1999, the Defense Information Systems Agency certified 23 of 34 mission-critical systems as Y2K compliant; 7 were still in the development phase and had not been tested, and 4 had been terminated. All of the systems that were reviewed had interface agreements, where required, and incorporated the Y2K references in contracts for commercial hardware and software. However, two systems did not have the required contingency plans because the project managers had not insisted on approved contingency plans from the U.S. Army Communications and Electronics Command for both systems. Without contingency plans for these systems it could adversely affect the ability to complete mission requirements should a Y2K problem materialize.

It was recommended that the Director, Defense Information Systems Agency, develop contingency plans for the Defense Satellite Communications System and the Defense Information System Network Deployed (Step) Switch Multiplexer Unit System.

Both the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), and the Inspector General, Defense

Information Systems Agency, concurred with the recommendation. The Inspector General, Defense Information Systems Agency, stated that contingency plans for both the Defense Satellite Communications System and the Defense Information System Network Deployed (Step) Switch Multiplexer Unit System were being prepared and would be completed by June 20, 1999.

Report No. 99-199, "Year 2000 Conversion Program for Defense Critical Suppliers," July 2, 1999. The report stated that in an effective outreach effort under the overall leadership, direction, and guidance of the Defense Logistics Agency and the Joint Supplier Capability Working Group, nearly 5,000 Defense critical suppliers were identified and about 4,500 assessed for Y2K compliance. Critical supplier assessments were, for the most part, conducted within the guidelines established in the Y2K Supplier Capability Assessment Guide. However, the Inspector General, DoD, observed and addressed certain inconsistencies in assessment methodologies and resource applications that, if not corrected, could have jeopardized the timely and accurate supplier assessment and mitigation process. Specifically:

- The Defense Industrial Supply Center-Philadelphia initially did not recommend follow-up assessments for suppliers that indicated that they would not be Y2K compliant until late in calendar year 1999. Of the 406 assessments reviewed, 38 assessments had indicated some future date for total Y2K compliance, yet no follow-up action was suggested. The DLA agreed to query the supplier assessment database to determine whether the issue was found throughout the completed assessments. Future actions will include a follow-up with the suppliers and a change in the previously assigned supplier risk.
- The Defense Contract Management Command-Reading did not perform on-site assessments for all suppliers ranked highly critical. Of the 42 suppliers assigned to them, 24 were ranked highly critical, but only 14 of those 24 suppliers were assessed on-site. Management assured Inspector General, DoD, that on-site assessments would be accomplished for the 10 remaining suppliers.
- The Navy did not begin its assessment of 785 assigned suppliers until April 14, 1999. The original milestone date for the completion of all supplier assessments was April 30, 1999. The Inspector General, DoD, observed that the Navy neither had adequate resources identified nor the time to complete the assessments by April 30. The Defense Contract Audit Agency assumed responsibility for over 200 of the Navy supplier assessments. Additional personnel were assigned to the assessment effort.

Report No. 99-197, "Status of Resources and Training System Year 2000 Issues," June 29, 1999. The report stated that the Defense Information Systems Agency (DISA) appropriately certified and reported the Global Status of Resources and Training System as Y2K compliant. However, DISA inappropriately certified and reported the Status of Resources and Training System database as Y2K compliant. The Army met the Y2K certification criteria for the Global Command and Control and Control System-Army, but the

system was not certified in accordance with the Army certification criteria. The Navy appropriately certified the Global Command and Control Systems-Maritime as Y2K compliant. The Air Force did not include the Air Force Status of Resources and Training System Data Entry Tool on the DoD Y2K reporting database. Also, DISA did not include the Global Online Marine Edit and Report System on the DoD Y2K reporting database. As a result, the Services' ability to report unit resources and training status in a Y2K environment was not assured.

Neither the Joint Staff nor the Office of the Under Secretary of Defense for Personnel and Readiness had conducted or planned to conduct end-to-end Y2K testing of the readiness reporting function. As a result, neither the Joint Staff nor the Office of the Under Secretary of Defense for Personnel and Readiness knew whether unit readiness information reported to the National Command Authorities, and contained in the Joint Operation Planning and Execution System database, would be complete and accurate after January 1, 2000. In addition, the Status of Resources and Training System user may not have access to the readiness status of combatant units after 1999.

The Joint Staff did not initiate development of an operational contingency plan for the DoD readiness reporting function and the Army, Air Force, and DISA did not prepare adequate system contingency plans. Without adequate contingency plans, DoD could not minimize the adverse effects of Y2K disruptions such as loss of data or communications, and ensure that it had alternative ways to continue military planning operations.

The report recommended that the Director, Defense Information Systems Agency:

- recertify the database of the Status of Resources and Training System until the system is fully tested for Y2K compliance in accordance with the DoD Y2K Management Plan,
- designate the Global Inline Marine Edit and Report System as a mission-essential system and perform all tests and certifications recommended for mission-essential systems contained in the DoD Y2K Management Plan,
- prepare a system contingency plan for the Global Online Marine Edit and Report System, and
- prepare a system contingency plan for the Status of Resources and Training System database and Global Status of Resources and Training System.

The report further recommended that the Director, U.S. Army Information Systems for Command, Control, Communications, and Computers, certify that all required Y2K tests have been performed on the Global Command and Control System-Army and that the system is Y2K compliant. In addition, the report recommended that the Director, Air Force Air and Space Operations Directorate of Operations and Training, designate the Air Force Status of

Resources and Training System Data Entry Tool as a mission-essential system and to perform all test and certifications recommended for mission-essential systems contained in the DoD Y2K Management Plan.

Additionally, the report recommended that the Under Secretary of Defense for Personnel and Readiness and the Director, Joint Staff:

- develop an operational readiness assessment for the readiness reporting function, and
- coordinate the planning and execution of readiness reporting functional area Y2K end-to-end testing with the Defense Information Systems Agency and the Services.

The report also recommended that the Director, Joint Staff, in coordination with the Services and the Defense Information Systems Agency, expedite the preparation of an operational contingency plan for the DoD readiness reporting function.

DISA stated that certification of Y2K compliance for the Status of Resources and Training System was complete as of April 30, 1999. DISA concurred with the recommendation to designate the Global Online Marine Edit and Report System as a mission-essential system and to perform all test and certifications recommended by the DoD Y2K Management Plan. DISA stated that it had submitted Global Online Marine and Edit System test documentation to the Joint Interoperability Test Command for assessment, which is ongoing. DISA partially concurred with the recommendations to prepare system contingency plans for the Global Online Marine Edit and Report System, the Global Status of Resources and Training System, and the Status of Resources and Training System database. It stated that the final system contingency plan incorporating those systems is awaiting signature. The Office of the Under Secretary of Defense for Personnel and Readiness and the Joint Staff concurred with the recommendations to develop an operational readiness assessment for the readiness reporting function and to coordinate the planning and execution of a readiness reporting functional area Y2K end-to-end test.

The Joint Staff concurred with the recommendations to develop an operational contingency plan and to develop system contingency plans in accordance with the DoD Y2K Management Plan for the Global Command and Control System-Army and the Air Force Status of Resources and Training System Data Entry Tool. The Joint Staff and DISA expect to accomplish those tasks by July 1999. Comments from the Air Force have still not been provided and action is ongoing.

Report No. 99-196, "Year 2000 Computing Issues Related to Health Care in DoD – Phase II," June 29, 1999. The report stated that the Office of the Assistant Secretary of Defense (Health Affairs) and the Military Departments continued making progress in identifying and correcting the Y2K problem in Military Health System automated information systems, biomedical devices, and facility devices. However, further actions by the Office of the Assistant Secretary of Defense (Health Affairs) are needed. Specifically, actions in the

biomedical device area should include increasing oversight of noncompliant biomedical devices by including contingency plan requirements in monthly reports and by expediting the implementation of Y2K Readiness Assessment Team Evaluations. Actions should also include establishing a deadline for removal of noncompliant devices and improving the reporting of compliant biomedical devices by disclosing varying methodologies of data collection. In addition, based on audit work at two Navy medical centers, the accuracy of Navy noncompliant biomedical device reports needed improvement. Actions are necessary to minimize the risk that DoD will not realize full health care and medical readiness capabilities due to Y2K related issues.

The report recommended that the Assistant Secretary of Defense (Health Affairs):

- increase oversight of noncompliant biomedical devices by expanding monthly status reporting to include whether contingency plans exist for each device, and expediting the implementation of Y2K Readiness Assessment Team Evaluations;
- establish a deadline that provides sufficient time for the removal of noncompliant biomedical devices from service before the year 2000;
- improve the reporting of compliant biomedical devices by disclosing varying methodologies of data collection used; and
- increase the accuracy of Navy noncompliant biomedical device reports to senior management by reconciling the medical logistics chief and military treatment facility databases.

The Military Health System Chief Information Officer concurred with the findings and recommendations and is taking action. A deadline prior to January 1, 2000, will be established for the removal of noncompliant biomedical devices based on the status of remediation efforts and consideration of risk to patient care due to the removal of functioning equipment in advance of its known date of failure. Military Treatment Facility personnel will improve the accuracy of Navy noncompliant biomedical device reports through the creation of a centralized web-enabled database. The presentation of compliant biomedical devices will be improved by providing briefing material that specifically discloses the differences in Military Department data collection methodologies. Finally, the report commends the staff's aggressive and proactive approach to resolving Y2K related issues. There are no outstanding issues from the report.

Report No. 99-194, "Year 2000 Conversion Program at the Army National Guard," June 29, 1999. The report stated that 5 of the 11 National Guard mission-critical systems had not met the Office of Management and Budget's compliance deadline of March 31, 1999. Four of the five systems were compliant by June 1999. However, the systems contingency plans did not address continued operations of the National Guard. In addition, the National Guard did not have plans or a schedule for testing the contingency plans. The National Guard had made progress in ensuring that its Communications

Operational Contingency Plan could be implemented if communications failed as a result of Y2K disruptions, but needed to do more work on other operational contingency planning.

The report recommended that the Director, Army National Guard:

- update the risk management plans to include how a system or device may fail and how the failure will affect the system function or mission and the functions and missions of interfacing systems;
- update the system contingency plans to include sufficient system details, resource requirements, degraded system functionality, impacts to hardware and software, and detailed solutions and workarounds;
- prepare a schedule to complete the analysis of mission-critical functions and complete the operational contingency plans; and
- prepare test plans and schedule a test in a functional or operational exercise once the contingency plans are updated and prepared.

The Director, Army National Guard, nonconcurred with the finding that a revised or rephased test plan was needed and the assessment of risk of failure of the Communications Operational Contingency Plan. Officials stated that recent results demonstrated a high-degree of success in the communication plan. As a result, the finding has been revised. The Assistant Secretary of Defense (Command, Control, Communication and Intelligence) supported the finding and recommendations. The Assistant Secretary also stated that his office had reviewed and was satisfied with the National Guard progress in correcting the identified deficiencies, especially those pertaining to the operational contingency plans. He stated that funding remained as a concern. The Director, Army National Guard, concurred with the findings and stated that the last system would be certified by September 1999.

Management also provided updated information on the mission-critical systems identified in the report. Only one system is not compliant. Some recommendations were revised and action is still ongoing.

Report No. 99-190, "Year 2000 Compliance of the Worldwide Port System," June 18, 1999. The report stated that the Worldwide Port System had a low-risk of failure associated with the Y2K processing. The Worldwide Port System program manager implemented a certification process that verified and certified the Worldwide Port System in accordance with DoD and Army Y2K guidance. The program manager documented test plans and test results, established interface agreements for systems with which the Worldwide Port System interfaced, and prepared contingency plans before system certification. A contracted independent assessment concluded that the Worldwide Port System faces low-risk of Y2K disruptions. As a result, Worldwide Port System should be able to support operational requirements for tracking and documenting the movement for DoD ocean-bound cargo through water ports in a Y2K environment.

Report No. 99-189, “Year 2000 Compliance of the Standard Army Ammunition System-Modernization,” June 18, 1999. The report stated that the Program Executive Office for Standard Army Management Information Systems Y2K Project Office and the Project Manager for the Global Combat Support System-Army Project Office adequately planned for and managed Y2K risks for the Standard Army Ammunition System-Modernization. These offices took effective action to ensure that the Standard Army Ammunition System-Modernization was certified in time to participate in logistics end-to-end testing that was scheduled to begin in May 1999. The estimated completion date that a Y2K compliant Standard Army Ammunition System-Modernization would be implemented at all active Army units was June 1999.

Report No. 99-185, “Year 2000 Conversion Within the Defense Security Service,” June 11, 1999. The report stated that the Defense Security Service was behind the prescribed DoD schedule for Y2K conversion and needed to accelerate its effort. Areas of concern included: the Defense Security Service did not prepare system contingency plans, operational contingency plans, or an end-to-end test plan to make an operational readiness assessment of its personnel security investigative and industrial security programs.

Additionally, the Defense Security Service test plan did not have sufficient detail to adequately test its mission-essential systems for Y2K compliance. During the audit, management took action to address deficiencies in system status, reporting and interface agreements.

The report recommended that the Director, Defense Security Service:

- prepare system contingency plans for the 15 Defense Security Service mission-essential systems lacking plans;
- prepare operational contingency plans for the Defense Security Service headquarters; the Operations Centers at Linthicum, Maryland, and Columbus, Ohio; the Security Research Center; the Department of Defense Polygraph Institute; the 13 operating locations; and the field security investigative function;
- revise the Defense Security Service test plan to address Y2K compliance testing required for each mission-essential system, using the DoD Y2K Management Plan, as the framework for the revised test plan;
- complete the retesting of previously tested systems that lacked formal documentation and certification and test the remaining Defense Security Service mission-essential systems; document test results for all systems; and certify all systems as Y2K compliant on successful completion of the test; and
- provide the end-to-end test plan to the Y2K Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) for review of technical adequacy.

The Director, Defense Security Service, concurred with the findings and recommendations and took corrective actions. Management plans to finalize Defense Security Service system and operational contingency plans by September 30, 1999. In addition, Defense Security Service plans to revise its test schedule to reflect new milestone dates for system and end-to-end testing. Corrective actions are still ongoing.

Report No 99-182, "Defense Information Systems Agency Management of Mainframes," June 9, 1999. The report stated that DISA and the Central Design Activities have made significant progress in identifying and renovating the domains at the Defense Megacenters. From December 1998 to April 1999 the number of compliant domains increased from 159 to 258. However, additional work is needed to lower the risk of Y2K related failures. As of March 31, 1999, DISA had 94 domains identified as noncompliant. Forty percent of the noncompliant domains are shared among Military Departments and Defense Agencies, causing risks to applications that share noncompliant domains.

The report recommended that the DoD Principle Director Year 2000:

- meet with the Central Design Activities for the applications that share a noncompliant domain to review the status and necessary action to renovate the domains; and
- determine whether to classify noncompliant applications, which share domains with mission-critical applications, as mission critical or mission essential.

In addition, the report recommended that the DoD Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), establish a policy to remove, by the start of FY2000, noncompliant applications, executive software, and hardware from any mainframe domain shared by a compliant application, even if the compliant application belongs to the same Military Department or Defense Agency.

The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that the DoD Principal Director for Y2K has taken action to ensure adequate review of the status of the Defense Megacenter domains. Also, the DoD Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), plans to establish a policy to remove noncompliant products providing that the removal of the noncompliant products from shared domains does not adversely impact mission support capability.

Intensive management, including the OSD involvement continues to be warranted until all domains are compliant to include a drop dead date for noncompliant products and applications in a shared domain. Action for the report is complete and no further action is required.

Report No. 99-181, "Year 2000 Issues Relating to Security Assistance and Foreign Military Sales," June 9, 1999. The report stated that the Defense Security Cooperation Agency and the Military Departments used adequate

processes to notify foreign military sales customers about the Y2K compliance status of items purchased through the foreign military sales program. The Army sent written notification to DoD security assistance organizations identifying all known noncompliant Army systems and equipment purchased through the program. As of April 15, 1999, the Navy sent more than 300 notification letters to security assistance organizations and summarized the results in a matrix to allow for tracking and response. The Air Force identified all known equipment sold to foreign military sales customers and developed a report on the Y2K status of foreign military sales systems. Because of those efforts, the risk of disruption of interoperability with U.S. allies will be reduced.

Report No. 99-179, "Status of Year 2000 Compliance at the Defense Commissary Agency," June 7, 1999. The report stated that the Defense Commissary Agency was making progress in its Y2K conversion efforts, but more could be done to minimize the risk. The Defense Commissary Agency target certification date for the Defense Commissary Agency Interim Business System may not allow sufficient time to correct unexpected errors, changes, and delays in solving Y2K issues. As of April 9, 1999, the Defense Commissary Agency had identified the Y2K compliance status of only 55 percent of vendor infrastructure equipment critical to the operation of the individual commissaries and administrative offices. The contingency plan for the Defense Commissary Agency Interim Business System was inadequate, and the contingency plan for the infrastructure equipment was incomplete.

The report recommended that the Director, Defense Commissary Agency:

- expand the contingency plan for the Defense Commissary Agent Interim Business System to delineate alternative operation procedures that will be used to perform its functions if a system fails as a result of the year 2000;
- expand the contingency plan for the Defense Commissary Agency Interim Business System to delineate the operational procedures by which the mission or function supported by the system will be continued during a prolonged disruption of the system;
- complete contingency plans for each critical infrastructure equipment category that identifies alternatives actions to be taken at Defense Commissary Agency offices and commissaries if infrastructure equipment fails as a result of the year 2000; and
- test the contingency plans in the above recommendations to ensure that the alternative procedures are realistic and executable.

The Executive Director for Support, Defense Commissary Agency, concurred and stated that the Defense Commissary Agency has expanded the contingency plans to delineate alternative operational procedures if the Defense Commissary Agency Interim Business System and infrastructure equipment is disrupted by Y2K related issues. The Defense Commissary Agency is currently testing or planning to test the contingency plans to ensure the alternative procedures are realistic and executable. As of May 10, 1999, the Defense Commissary

identified the Y2K compliance status of 79 percent of vendor models of infrastructure equipment. The first two recommendations are closed and follow-up on the other recommendations is planned in mid-September 1999.

Report No. 99-176, "Impact of Year 2000 Issues on the Aegis Weapon System," June 2, 1999. The report stated that the Aegis Program Office took positive action towards ensuring that Y2K related issues would not disrupt the Aegis weapon system. The Aegis Program Office management ensured that:

- tests were planned and executed in accordance with the Navy Master Test Plan,
- comprehensive initialization procedures were developed,
- external interfaces were identified and memorandums of agreement were prepared,
- the Aegis weapon system was properly certified year 2000 compliant (September 17, 1998), and,
- year 2000 issues were effectively coordinated with other organizations.

However, the Aegis Program Office prepared a contingency plan that did not fully address risk assessments and key elements in the Navy Y2K Guidance Package. When these matters were brought to management's attention, it took immediate action to address risk assessments and revise the contingency plan.

Report No. 99-172, "Year 2000 Status of the Army Total Asset Visibility System," May 28, 1999. The report stated that the Army Total Asset Visibility System was prematurely certified Y2K compliant. However, it was neither tested in a Y2K compliant environment nor went through interface testing. The Army Total Asset Visibility system contingency plan was incomplete and had not been distributed to and coordinated with the functional users. As a result, without rigorous system testing and certification process and a comprehensive contingency plan, the functionality provided by the Army Total Asset Visibility system remains at risk of failure.

The report recommended that the Commander, Army Logistics Support Activity:

- recertify the Army Total Asset Visibility system with the following changes:
 - discuss the interface testing completed;
 - require a supporting test plan and results that are dated and signed by the testing official; and

-
- complete the certification checklist and note the results of external interface testing completed, rather than responding “not applicable.”
 - write a contingency plan, to be signed and dated by a responsible official, that includes:
 - a description of the basic interfaces;
 - identification of contingency plan trigger dates, activities, strategies, and procedures to be performed at specified dates or events;
 - a detailed description of manual procedures to be performed;
 - a discussion of the acceptable level of performance and the risk arising from the use of manual procedures; and
 - a plan to test the contingency plan itself.
 - coordinate the contingency plan with the functional users and all involved with making the plan work and distribute copies of the plan to all interested parties.

Additionally, the report recommended that the Army Chief Information Officer, adjust the OSD Y2K database and report to OMB to indicate that the Army Total Asset Visibility system is in validation phase and not certified as Y2K compliant, if the recertification of the Army Total Asset Visibility system is not completed by the next quarterly status report to OSD. Further, the report recommended that the Army Chief Information Officer, alert the Director, Logistics Systems Modernization, that the Army has not completed the systems certification testing requirements. The report also recommended that the Director, Logistics System Modernization, use the Army Total Asset Visibility contingency procedures in the Logistics end-to-end test, instead of using the Army Total Asset Visibility system and require the Army to sufficiently test the contingency procedures beforehand.

The Army concurred with the recommendation covering improvements to and coordination of the Army Total Asset Visibility contingency plan. The Army stated that the certification checklist did not require interface testing because the Army Total Asset Visibility interfaces had no format changes. The Army believed that recertifying the Army Total Asset Visibility system would be impractical, and would deny participation in the OSD sponsored end-to-end logistics tests. The Army stated that the cost of starting over on the recertification process would be an additional \$34,148, which the Army did not consider to be a prudent expenditure.

In response, the report stated that contrary to the Army stated position, the DoD Y2K Management Plan requires interface testing before certification. The report stated the end-to-end test events should not be used in lieu of required system certification testing requirements. The report recommended that the

Army alert the Director, Logistics Systems Modernization, that the Army Total Asset Visibility system did not go through proper certification testing and that he use the Army Total Asset Visibility contingency plan instead of using the Army Total Asset Visibility system in the Logistics end-to-end test. Finally, the report requires that the Army test its contingency plan before it is used in the Logistics end-to-end test.

The report requested comments by June 9, 1999, from the Army Chief Information Officer, Y2K Office and the Deputy Under Secretary of Defense (Logistics). Not all comments have yet been received and action is ongoing.

Report No. 99-171, "Space and Naval Warfare Systems Commands Preparations for Year 2000 Battle Group Systems Integration Testing," May 26, 1999. The report stated that the Space and Naval Warfare Systems Command took action to address Y2K compliance by establishing the Y2K War Room to coordinate Y2K management activities and developing a comprehensive timeline summary to monitor and track the installation of Y2K renovations. However, the Space and Naval Warfare Systems needed to improve their processes for preparing the *U.S.S. Constellation* Battle Group Systems Integration Testing for Y2K issues. The Space and Naval Warfare System Command must install and test systems that were not renovated and installed in time for the *U.S.S. Constellation* Battle Group Systems Integration Testing. The Space and Naval Warfare System Command initialization procedures did not address all required elements. The contingency plans did not provide specific procedures and a contingency plan was not developed for the Contingency Theater Automated Planning System.

The report recommended that the Commander, Space and Naval Warfare Systems Command, develop an effective review process for initialization procedures and develop a more effective quality assurance process to review the completeness of all contingency plans in accordance with the Navy Y2K Project Office contingency plan guidance. The report also recommended that the Contingency Theater Automated Planning System Program Manager develop a contingency plan that fully addresses the preparation, planning, and overview elements of the Navy contingency plan guidance.

The Navy concurred with all recommendations. All of the required initialization procedures have been completed and submitted to NAVSEA. The contingency plans reviewed during the audit have been updated; approved, using Space and Naval Warfare Systems Command's contingency plan review process; and submitted to CINC, U.S. Pacific Fleet. The Contingency Theater Automated Planning System initialization procedure was completed and forwarded to NAVSEA on July 20, 1999. In addition, the Contingency Theater Automated Planning System contingency plan was completed and forwarded to CINC, U.S. Pacific Fleet on July 21, 1999. Twenty-one of the Space and Naval Warfare Systems Command contingency plans are going through the Space and Naval Warfare Systems Command internal review process and are estimated to be completed by August 31, 1999.

Report No. 99-170, "Year 2000 Contingency Plans for Surface Ship Hull, Mechanical, and Electrical System," May 24, 1999. The report stated that

Integrated Information System Engineering Group, Naval Sea Systems Command, prepared initialization procedures for system operators to use in the Y2K rollover and implemented a Y2K certification test checklist. However, the contingency plan for the hull, mechanical, and electrical systems did not clearly show the link implementing the contingency plan with the procedures outlined in the engineering operational sequencing system. The contingency plan did not provide procedures to recognize system degradation, to detect corrupt system data, and to preserve and protect data.

The report recommended that the Director, Integrated Information Systems Engineering Group, Naval Sea Systems Command, establish a more effective quality assurance review process to ensure that contingency plans meet the Navy Y2K contingency and continuity-of-operations planning guide criteria. In addition, the report recommended that the Director, Integrated Information Systems Engineering Group, Naval Sea Systems Command, revise the hull, mechanical, and electrical contingency plans that did not adequately address the overview, planning, and preparation elements specified in the Navy Y2K contingency and continuity-of-operations planning guide.

The Navy concurred with the recommendations and stated that the Integrated Information Systems Engineering Group has begun strengthening its quality assurance review process, and the contingency plans for the hull, mechanical, and electrical systems have been revised and submitted for fleet review. Action completed includes improving the quality assurance review process and revising all contingency plans.

Report No. 99-169, "Year 2000 Compliance of the Navy Pioneer Unmanned Aerial Vehicle," May 24, 1999. The report stated that the Navy Pioneer Unmanned Aerial Vehicle is Y2K compliant and does not use mission-critical date or time entries relating to the year 2000. The Navy Pioneer Unmanned Aerial Vehicle received an inappropriate certification level, which resulted in it going through a validation phase that was not strictly necessary. However, the validation testing provided extra assurance that the system is Y2K compliant.

Report No. 99-168, "Year 2000 Compliance of the Navy Theater Mission Planning Center," May 24, 1999. The report stated that Navy Theatre Mission Planning Center system (both hardware and software) was appropriately certified Y2K compliant in December 1998. The program manager followed the Navy certification process and documented the system verification, testing, interfaces, and contingency plan before certification. In March 1999, the implementation of the Theater Mission Planning Center system was completed at Navy cruise missile support activities.

Report No. 99-167, "Year 2000 Compliance of the *Trident* Submarine Command and Control System," May 24, 1999. The report stated that the *Trident* Submarine Command and Control System, revisions 5.5 and 6.3 were certified Y2K compliant in September 1998. The program manager followed the Navy certification process and documented the system verification, testing, interfaces, implementation, and contingency plan. Thirteen of the 18 *Trident*

submarines have completed the implementation of the command and control system revisions 5.5 and 6.3, and the remaining 5 submarines are on schedule for completion.

Report No. 99-165, "Year 2000 Compliance of the Standard Army Maintenance System-Rehost," May 24, 1999. The report stated that the Program Executive Office for Standard Army Management Information Systems Y2K Project Office and the Project Manager for Global Combat Support System-Army Project Office adequately supported the March 29, 1999, certification of Y2K compliance of the Standard Army Maintenance System-Rehost system by assessing risks, testing for Y2K compliance, and preparing interface agreements and contingency plans.

Because of resource constraints, the DoD Y2K Management Plan's established milestone date for implementation was exceeded. However, the Program Executive Office for Standard Army Management Information Systems took effective action to ensure that the Standard Army Maintenance System-Rehost was certified in time to participate in logistics end-to-end testing that was scheduled for April 1999. The Y2K project officer of the Program Executive Office for Standard Army Management Information Systems estimated that a Y2K compliant Standard Army Maintenance System-Rehost system would be implemented at all active Army units by April 30, 1999, and at Army National Guard and Reserve units by September 30, 1999.

Report No 99-164, "Year 2000 Conversion Program for the Pentagon and DoD Leased Facilities," May 21, 1999. The report stated that the General Services Administration (GSA) and the Washington Headquarters Services were taking action to assess the risk of the Y2K problem for leased facilities that they manage for DoD and the Washington Headquarters Service took action to determine the Y2K compliance status of the Pentagon Reservation. However, GSA and the Washington Headquarters Service were limited in their actions and more action was needed. Lease agreements that they were operating under did not require the lessors to provide the Y2K status of the facilities, to provide an inventory of systems, or to test for Y2K compliance. Of the 384 facilities that GSA leases for DoD, lessors provided the Y2K status of only 161 facilities.

The report recommended that the Deputy Under Secretary of Defense (Installations) request that GSA hold regional meetings with building owners and provide DoD tenants of the 384 leased facilities with all available information on the Y2K status of those facilities and any recommended contingency measures.

The Deputy Under Secretary of Defense (Installations) nonconcurred with the recommendation, stating that DoD components are already responsible for ensuring that tenants in leased facilities receive the Y2K compliance information from the lessors or have suitable workarounds in place. The Deputy Under Secretary also stated that the report presumed that GSA has the ability to get the lessors to disclose the Y2K compliance status and that a letter to GSA will somehow make it possible for GSA to provide that information.

The Deputy Under Secretary was not fully responsive and did not provide any assurance that DoD tenants will be provided information on the Y2K status of

their leased facilities. The report recognizes that GSA cannot require the lessors to provide the Y2K status of their facilities. The intent of the recommendation was to provide DoD tenants of leased facilities with information on the Y2K status of those facilities. The Deputy Under Secretary needs to ensure that DoD tenants in leased facilities are notified of the Y2K status of the buildings and recommended contingency plans.

Management comments on the final report were received on July 21, 1999. Management took the actions necessary and included a copy of the letter that management sent to the General Services Administration requesting that they take the action that was recommended. There are no outstanding issues.

Report No. 99-163, "Year 2000 Issues within the U.S. Pacific Command's Area of Responsibility Host Nation Support to U.S. Forces Korea," May 17, 1999. The report stated that the U.S. Forces Korea had not obtained interface agreements or formal assurances of Y2K compliance from Republic of Korea civil and military (government) organizations and commercially operated companies providing armistice and wartime host nation support. More efforts are needed to minimize the risk of disruption to the Republic of Korea/U.S. Combined Forces Command mission to stabilize the political situation on the Korean peninsula, to plan for the defense of the Republic of Korea and, in the case of hostilities, to direct Republic of Korea/U.S. combat forces to defeat enemy aggression.

Following briefings on initial audit results, management took immediate corrective actions. On February 26, 1999, the U.S. Forces Korea invited Republic of Korea Ministry of National Defense and Republic of Korea Joint Chiefs of Staff officials to become full members of the U.S. Forces Korea Y2K Steering Group to discuss mutual Y2K efforts. On March 5, 1999, a meeting was held to coordinate the Y2K issues between the Republic of Korea and U.S. Forces Korea. Because of the immediate corrective actions taken, the report contained no recommendations.

Report No 99-162, "Year 2000 Status of the Advanced Medium Range Air-To-Air Missile," May 17, 1999. The report stated that the Air-To-Air Joint Systems Program Office ensured Y2K compliance of the Advanced Medium-Range Air-To-Air Missile by effectively assessing Y2K issues. The Advanced Medium-Range Air-To-Air Missile does not require a specific weapon system Y2K contingency plan because it does not contain or process dates. Raytheon Systems Company developed a contingency plan and plans to monitor Y2K issues to sufficiently support the operation and deployment of the Advanced Medium-Range Air-To-Air Missile. The Advanced Medium-Range Air-To-Air Missile has a low-risk of being disrupted by Y2K related issues. The Navy inaccurately reported the Advanced Medium-Range Air-To-Air Missile Captive Equipment Pod as a mission-critical Navy system in the Naval Y2K database. The Chief Information Officer, Navy, deleted it from the database because it is not a mission-critical system, nor is it a Navy system.

Report No. 99-161, "Year 2000 Computing Issues Related to the Defense Fuels Automated Management System," May 17, 1999. The report stated that the Defense Logistics Agency has established a Y2K program management

office, which provides direct oversight of the entire Defense Logistics Agency Y2K effort. However, the renovated Defense Fuels Automated Management System programs were not tested on a domain that was Y2K compliant. The Defense Energy Support Center had not developed contingency plans that identified methods for conducting operations in the event Defense Fuels Automated Management System suffered a Y2K disruption. As a result, test results may not reflect Defense Fuels Automated Management System actual Y2K performance. In addition, incomplete contingency plans could lengthen the time before operations could resume if Y2K related disruptions occur.

The report recommended that the Director, Defense Logistics Agency, assess the risk associated with testing the renovated Defense Fuels Automated Management System program on a non-Y2K compliant test domain. Based on the results of the risk analysis, determine the need to retest Defense Fuels Automated Management System programs. The report also recommended that the Director, Defense Information System Agency, develop operational contingency plans for the Defense Fuels Automated Management System. Additionally, the report recommended that the Director, Defense Logistics Agency, in conjunction with the Director, Defense Information Systems Agency, ensure that the test domain is Y2K compliant before the certification of the Defense Fuels Automated Management System as Y2K compliant. DISA and DLA issued comments and concurred with all of the recommendations. All issues were resolved and action is completed for the first two recommendations and action is ongoing between DLA and DISA to ensure that the test domain is Y2K compliant before certification. Estimated completion date for this is August 31, 1999.

Report No. 99-158, "Year 2000 Status of the AN/ARC-220 Nap-of-the-Earth Aircraft Communication System," May 14, 1999. The report stated that the program manager took necessary precautions to assure that the AN/ARC-220 Nap-of-the-Earth Aircraft Communication System will be Y2K compliant. The program manager properly certified the system and developed an adequate contingency plan. The system is at low risk and should operate successfully in the year 2000. A higher level of test for the AN/ARC-220 is not required because the system is not date dependent.

Report No. 99-157, "Year 2000 Compliance of the Standoff Land Attack Missile," May 14, 1999. The report stated that the Standoff Land Attack Missile System, baseline version, was certified as Y2K compliant November 1998. The three interface systems were appropriately certified Y2K compliant in December 1998 and March 1999. The Standoff Land Attack Missile B/L program executive officer followed both the Navy and the DoD Y2K certification process.

Report No. 99-151, "Year 2000 Conversion Program for the Air Force Reserve," May 11, 1999. The report stated that the Air Force Reserve was proactive in its Y2K conversion effort. During the audit, the Air Force Reserve developed interface agreements and a contingency plan for the Improved Weather Reconnaissance System. However, two of four Air Force Reserve Wings that were reviewed did not make adequate progress in assessing the Y2K status of infrastructure systems and preparing contingency plans. This is

because of the Air Force Reserve units not adequately emphasizing and addressing the DoD Y2K Management Plan in solving Y2K issues.

This report recommended that the Commander, Air Force Reserve Command, require the 482d Fighter Wing and the 440th Airlift Wing to:

- determine whether their infrastructure systems are mission critical, evaluate Y2K compliance, and document the results,
- establish a schedule for infrastructure system compliance,
- revise the contingency plans for the 482d Fighter Wing and 440th Airlift Wing to recognize date-dependent systems, assign risks, and identify alternative solution and workaround, and
- review and report on system compliance and completion of contingency plans.

The Chief of Air Reserve concurred with the findings and recommendations. Aside from recommending a minor text change, the Chief of Air Reserve stated the 482d and 440th had taken action and provided the actual or estimated completion dates for each recommendation.

Report No. 99-146, “Year 2000 Compliance of the *Seawolf*-Class Submarine Combat System,” May 3, 1999. The report stated that the *Seawolf*-Class Submarine Combat System (AN/BSY-2) was certified as Y2K compliant for both software and hardware in December 1998 using the DoD and Navy guidance. Before certification, the combat system program manager documented the system verification, testing, interfaces, implementation, and contingency management plan. As a result, the Navy has minimized the Y2K failure of the *Seawolf*-Class Submarine Combat System. The AN/BSY-2 software upgrade is on schedule to be implemented on the *Seawolf*-Class submarines.

Report No. 99-145, “Year 2000 Issues within U.S. European Command and its Service Components,” April 30, 1999. The report stated that the U.S. European Command was making progress in addressing its Y2K problems. However, for a successful conversion, the U.S. European Command and its Service Component needed to take additional precautions.

The report recommended that the Commander in Chief, U.S. European Command, through the U.S. European Command Year 2000 Task Force and in coordination with its Service Component Y2K office:

- ensure that users of the Carnegie Mellon database have the appropriate equipment that allows them to access the database;
- complete system architectures to determine Y2K status for all mission-critical functional areas,

-
- coordinate with the Military Department medical commands, the Office of the Assistant Secretary of Defense (Health Affairs), and the U.S. Transportation Command to obtain the Y2K status of health care systems used in the European theater,
 - prepare all required operational contingency plans by March 31, 1999,
 - include aircraft and weapon systems in the operational evaluation,
 - issue guidance for uniformity addressing host nation infrastructure issues in the theatre,
 - establish a central office within the European theater for maintaining Y2K compliance data on host nation infrastructure, and
 - identify and validate Y2K funding requirement.

This report also recommended that the Assistant Secretary of Defense (Command, Control, Communication, and Intelligence) issue and distribute a users' manual for the Carnegie Mellon data base and a policy on the roles and responsibilities of the unified commands in addressing configuration management year Y2K issues.

In addition, the report recommended that the Army Y2K Program Office, issue operational contingency planning guidance. Finally, the report recommended that the Joint Staff modify operational evaluation guidance to clarify the scope of operational evaluations and initiate action to invite the North Atlantic Treaty Organization to participate in the U.S. European Command operational evaluation.

The U.S. European Command took the following responsive actions:

- distributed the Carnegie Mellon database to its Service Components via email,
- completed the system architectures needed for the operational evaluation,
- planned to have all operational contingency plans completed by September 30, 1999,
- planned to issue guidance on host nation support in August 1999,
- designated the task force as the central office for maintaining Y2K compliance data on host nation support, and
- identified Y2K funding requirements.

The OASD (C³I) stated that it would work database access problems on a case-by-case basis. In addition, the Director, Joint Staff, has proposed to the

OASD (C³I) Senior Official their version of the DoD overarching policy on configuration management of Y2K operational evaluations. OASD (C³I) has disseminated the Joint Staff Configuration Management Plan for coordination with the Defense Agencies and the DoD Intelligence Community for comments. Once the coordination is complete, the Configuration Management Plan will be modified to address the complete DoD wide Y2K operational evaluations, integration testing, and functional end-to-end testing issues. As of August 11, 1999, no final decisions have been made regarding policy for Configuration Management.

Report No. 99-144, "Guidance for the DoD Year 2000 Quarterly Report," April 30, 1999. The report stated that although there have been improvements since the 1997 Department of Defense Inspector General audit, the November 1998 and February 1999 DoD Y2K Quarterly Reports to OMB still contained inaccurate and unreliable data, largely because of the need for manual compilation of the report in a condensed timeframe. The number of the errors were not sufficient or material enough to distort the overall DoD Y2K conversion status.

In December 1998, the Senior Civilian Official, OASD (C³I), revised the DoD Y2K Management Plan to simplify reporting requirements by discontinuing the requirement to report nonmission-critical systems and clarified the OASD (C³I) responsibility for the accuracy of the DoD Components' Y2K data. The OASD (C³I) plans to discontinue manual data consolidation procedures and to use the OSD Y2K database for preparing the DoD Y2K Quarterly Report to OMB. This should reduce the discrepancies.

Report No. 99-143, "Preparation of the Wide-Area Munition for the Year 2000," April 30, 1999. This report stated that the Wide-Area Munition Program Office developed adequate plans and management to comply with the requirements of the DoD Y2K Management Plan and the Army Y2K Compliance Checklist. The Wide-Area Product Improvement Program, a modification of a basic wide-area munition scheduled for product delivery after Y2K, will contain date processing functions and will be contractually required to be Y2K compliant. The Wide-Area Munition Program Office was actively planning and managing Y2K issues and complied with requirements of the DoD Management Plan. The Wide Area Munition Program Executive Officer appropriately certified both the basic Wide-Area Munition and the Wide-Area Munition Product Improvement Plan as Y2K compliant on May 3, 1998.

Report No. 99-141, "Year 2000 Issues Within U.S. Central Command and the Service Components," April 22, 1999. The report stated that United States Central Command (USCENTCOM) refined its Y2K conversion efforts and was making progress in addressing its Y2K problems. However, the levels of Y2K efforts within USCENTCOM and its Component commands varied in scope and were still evolving. To mitigate risk, USCENTCOM and its Component commands must intensify efforts.

The report recommended that the Commander in Chief, U.S. Central Command:

- continue to develop system contingency plans for all mission-critical systems;
- develop continuity of operation plan;
- require Component commands to use the thinline approach to identify mission-critical systems;
- require Component commands to report the status of mission-critical systems using the reporting criteria established by DoD;
- require Component commands to develop and document a system contingency plan for mission-critical systems and a continuity of operations plan, to include conducting risk assessments; and
- require Component commands to develop contingency plans for all support provided by host nations in the area of responsibility.

USCENTCOM concurred with the finding and recommendations and provided details on efforts to develop, acquire, and test system contingency plans, and develop continuity of operations plans. The Air Force and USCENTCOM's comments were fully responsive. The Army's comments concerning conforming its reporting of Y2K compliant systems to an established criteria and providing information on subordinate commands' Y2K status were nonresponsive. Comments from the Navy were partially responsive concerning information on vessel Y2K status.

Report No. 99-136, "Government-Furnished Equipment Year 2000 Issues for Army Chemical Demilitarization," April 16, 1999. The report stated that the Army Program Manager for Chemical Demilitarization took positive actions to address the Y2K problem by including Y2K compliance language in prime contracts for the construction of three stockpile disposal sites. However, the Army Program Manager failed to assess the inventory of Government-furnished equipment to determine the equipment's Y2K compliance and did not prepare assessment, contingency, and risk management plans. Also, he did not assess the Government-furnished equipment contracts to determine whether they needed to be modified to include Y2K compliance language. As a result, the Army's equipment and systems at the Anniston, Alabama; Umatilla, Oregon; and Pine Bluff, Arkansas, sites may not be Y2K compliant, increasing the risk of delayed completion of construction or operational problems after installation. The report recommended that the Army Program Manager for Chemical Demilitarization, prepare revised milestone dates for completing and assessing Government-furnished equipment and for preparing the required DoD planning documentation for the Pine Bluff, Umatilla, and Anniston disposal sites. Additionally, the report recommended that the Army Program Manager for Chemical Demilitarization prepare a schedule, with milestone dates, for correcting and testing the Government-furnished equipment that is adversely affected by the Y2K problem. The report recommended that the Army Program

Manager for Chemical Demilitarization, review planned purchases of equipment for Y2K issues and take actions to ensure that Government-furnished equipment will be Y2K compliant.

The Deputy Assistant Secretary of the Army, Chemical Demilitarization, concurred with the recommendations and provided a schedule with milestone dates that outlines completing and assessing Government-furnished equipment. The Government-furnished equipment assessment was completed on March 31, 1999. The Deputy Assistant Secretary of the Army Chemical Demilitarization, stated that all three sites are reviewing each equipment procurement that is not yet complete for potential Y2K impacts. The review process should be complete by June 30, 1999. Planned purchases with potential Y2K impacts will contain the appropriate Y2K Federal Acquisition Regulation requirement for compliance. The original follow-up response was due on July 29, 1999, but the Army requested more time to provide a response. Estimated completion date is now August 26, 1999.

Report No. 99-134, "Year 2000 Compliance of Selected Air Mobility Command Systems," April 13, 1999. The report stated that the Air Mobility Command program managers had taken the necessary action to achieve Y2K compliance for the Command and Control Information Processing System and the Global Air Transportation Execution System. The Air Mobility Command management implemented a certification process that ensured systems were verified and certified. The Air Mobility Command "Year 2000 Certification Process" guidance requires a comprehensive verification of the system testing, interfaces, and contingency documentation before certification. Auditor improvement suggestions to the Global Air Transportation Execution System program office regarding its contingency plan were promptly incorporated. Air Mobility Command certification actions minimized the risk of failure associated with Y2K processing for the Command and Control Information Processing System and the Global Air Transportation Execution System.

Report No. 99-133, "Year 2000 Compliance of the Global Transport Network," April 13, 1999. The report stated that the U.S. Transportation Command certified the Global Transportation Network system as Y2K compliant on December 10, 1998. The Global Transportation Network program manager followed the U.S. Transportation Command certification process documented in its "Year 2000 Compliance Action Plan," which required a comprehensive verification of the system testing, interfaces, and contingency documentation before certification.

The "Year 2000 Compliance Action Plan" implemented DoD Y2K guidance to develop a Y2K compliance action plan and detailed the program management office's pursuit of Y2K compliance for the Global Transportation Network System. The Command complied with DoD and Air Force guidance in processing the Global Transportation Network system Y2K certification. Auditor improvement suggestions were promptly incorporated into the Global Transportation Network system procedures and documents. The program management office's adherence to the certification process minimized the risk of failure associated with year 2000 processing for the Global Transportation Network system.

Report No. 99-130, "Preparation of the Sense and Destroy Armor Munition for the Year 2000," April 12, 1999. The report stated that the Sense and Destroy Armor Munition Program Office was actively planning and managing Y2K issues. All documentation was being prepared as required by the DoD Management Plan and the Army Y2K Compliance Checklist. The Sense and Destroy Armor Munition contract had language from Federal Acquisition Regulation 39.106, "Year 2000 Compliance," and contained Y2K warranties of commercial and noncommercial supply items at no additional cost to the Government. No interface agreements were applicable.

Report No. 99-126, "Year 2000 Issues within the U.S. Pacific Command's Area of Responsibility Strategic Communications Organizations," April 6, 1999. The report stated that during September through December 1998, the selected strategic organizations visited had made some progress in addressing the Y2K problem, but the efforts to address the Y2K problem at the Naval Computers and Telecommunications Area Master Station-Pacific, aboard the *U.S.S. Blue Ridge*, and at 58th Signal Battalion varied in scope and were evolving. Those organizations generally still needed to:

- establish Y2K action plans and develop definitive risk reduction strategies,
- conduct risk assessments of the potential impact of the Y2K problem on operations,
- appoint Y2K working groups,
- complete the identification and inventory of global and nonglobal systems,
- complete the assessments of Y2K compliance and to prioritize mission-critical systems,
- develop contingency plans and continuity of operations plans, and
- identify and report resource requirements to implement Y2K efforts

These tasks were not completed because adequate DoD, Military Department, and Pacific Communication guidance was not promptly disseminated. Therefore, subordinate organizations did not effectively and promptly implement Y2K corrective guidance. Also, system operators did not always receive information on the Y2K status of systems or remediation schedules. As a result, assurance of timely and complete Y2K conversion for those organizations was still incomplete as of late 1998.

The report recommended that the Commander in Chief, U.S. Pacific Command:

- ensure that guidance is adequate to eliminate confusion in the assignment of responsibilities toward Y2K efforts;

-
- ensure that guidance is disseminated to all operational users involved in the Y2K effort; and
 - require Component commands with elements in the U.S. Pacific Command area of responsibility to assist the U.S. Pacific Command to ensure that guidance is adequate to eliminate confusion in the assignment of responsibilities for Y2K efforts and to disseminate that guidance to all operational users involved in the Y2K effort.

The report also recommended that the Commander, U.S. Army Pacific, and the Commander, U.S. Pacific Fleet, closely monitor and, where necessary, actively assist subordinate commands' efforts to:

- complete risk assessments of the potential impact of Y2K problems on operations;
- complete the identification or inventory of global and nonglobal systems;
- complete the assessments of Y2K compliance;
- complete the prioritization of mission-critical systems;
- develop or obtain contingency and continuity of operations plans; and
- identify and report resource requirements to implement Y2K efforts.

The Commander in Chief, U.S. Pacific Command; Commander, U.S. Army Pacific; and the Commander, U.S. Pacific Fleet; did not respond to the draft report, but did comment on the final report and concurred with the recommendations. Action is ongoing.

Report No. 99-125, "Year 2000 Issues within the U.S. Pacific Command's Area of Responsibility U.S. Forces Korea," April 7, 1999. The report stated that the U.S. Forces Korea made progress in addressing the Y2K problem. Some of their positive actions included establishing a Y2K Steering Committee and establishing the U.S. Forces Korea Y2K Working Group to collect and analyze data, and to track Y2K compliance. However, the level of effort within U.S. Forces Korea and its Component commands and supporting agencies varied in scope and was still evolving as of late 1998. Further, U.S. Forces Korea had not fully addressed the potential impact of Y2K problems on its ability to execute core missions and functions because U.S. Forces Korea had not:

- dedicated sufficient resources to Y2K efforts,
- adequately coordinated Y2K efforts with its Component commands and supporting agencies,

-
- fully identified and prioritized mission-critical systems, and
 - developed contingency plans for mission-critical systems and core missions and functions.

The report recommended that the Commander in Chief, U.S. Forces Korea:

- identify and dedicate sufficient resources to Y2K efforts;
- identify the systems and interfaces that are critical to core U.S. Forces Korea missions and functions;
- prioritize the fixes for U.S. Forces Korea's mission-critical systems and interfaces;
- develop or obtain system contingency plans for core missions, functions, and tasks;
- require Component commands and agencies with elements in Korea to assist U.S. Forces Korea in identifying the systems and interfaces critical to core U.S. Forces Korea missions, functions, and tasks; to assist in developing or obtaining system contingency plans for U.S. Forces Korea mission-critical systems; to assist U.S. Forces Korea in developing operational contingency plans for core U.S. Forces Korea missions, functions, and tasks; and
- require Component commands and agencies with elements in Korea to assign top priority to Y2K fixes for systems identified as U.S. Forces Korea mission-critical systems.

The Navy and DISA concurred with the findings and recommendations. DISA stated that the Commander, DISA, Korea and DISA, Pacific Area Command Field Office, would continue to provide Y2K support to U.S. Forces Korea in the areas identified. Comments on the final report were received from Commander in Chief, U.S. Forces Korea, the Commanding General, Seventh Air Force, and the Commander, Eighth U.S. Army. All issues have been resolved.

Report No. 99-124, "Year 2000 Compliance of the Counterintelligence/Human Intelligence Automated Tool Set," April 6, 1999. The report stated that the Counterintelligence/Human Intelligence Automated Tool Set hardware suite was appropriately certified as Y2K compliant in December 1998. The Counterintelligence/Human Intelligence program manager followed the Army certification process and documented the verification, testing, interfaces, and contingency documentation before certification of the Counterintelligence/Human Intelligence Automated Tool Set hardware suite. The Counterintelligence/Human Intelligence program office had completed distribution of Version 1 of the hardware suites and implementation of Version 2 upgrades to those hardware suites was on schedule. As a result, the Army has minimized the risk of Y2K failure of the Counterintelligence/Human Intelligence Automated Tool Set hardware suite.

Report No. 99-122, "Year 2000 Readiness Reporting," April 2, 1999. The report stated that the Joint Staff and the combatant commands lacked sufficient information to determine the Y2K readiness status of equipment for apportioned and assigned units. As a result, the National Command Authorities and the Chairman of the Joint Chiefs of Staff had incomplete information on the equipment status of combatant commands and may incorrectly assess the year 2000 deployability posture of apportioned and assigned units and organizations.

The report recommended that:

- the Director, Joint Staff, revise the Chairman of the Joint Chiefs of Staff Instruction 3401.02, "Global Status of Resources and Training System," October 20, 1997, and Joint Publication 1-03.3, "Joint Reporting Structure Status of Resources and Training System," August 10, 1993, to direct units to report in the Global Status of Resources and Training System the status of Y2K compliance of mission essential equipment and the affect of that compliance on their abilities to perform wartime missions.
- the Army Year 2000 Program Office, the Navy Year 2000 Project Office, the Air Force Year 2000 Office, and the Marine Corps Year 2000 Office, provide full descriptions to the Joint Staff, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), and the Inspector General, DoD, of their mechanisms for ensuring that the Y2K readiness status of apportioned and assigned units is reported to the combatant commands and the Joint Staff.

The Joint Staff did not provide comments on the final report. The Army, Navy, and Air Force nonconcurred with the recommendation to clarify what is being done to provide Y2K unit status data to the warfighters.

Report No. 99-118, "Marine Forces Reserve Preparation for Year 2000," March 31, 1999. The report stated that the Marine Forces Reserve is active in ensuring that its information systems and facility will be Y2K compliant. The Marine Forces Reserve has included the required clause in active contracts to ensure that it procured Y2K compliant information technology. In addition, the Reserve has initiated actions to assess system compliance, implemented corrective actions, and accurately reported the status of issues concerning potential Y2K related problems. As a result, the Marine Forces Reserve systems should be Y2K compliant if planned actions are accomplished.

Report No. 99-103, "DoD Efforts to Implement Year 2000 Compliance for Electronic Data Interchange," March 5, 1999. The report stated that the Military Services, the Defense Information Systems Agency, and the Defense Logistics Agency have made satisfactory progress in ensuring Y2K compliance for their electronic data systems. Twenty of 27 electronic data interchange systems identified were Y2K compliant and 1 system, believed to be compliant, was being tested. Four of the noncompliant systems were expected to be compliant in February 1999, one in March 1999, and two in May 1999.

Additionally, all 25 currently approved value added network providers had signed modified license agreements certifying that their systems were Y2K compliant.

Report No. 99-100, “Year 2000 Computing Issues: Defense Logistics Agency Distribution Standard System,” March 2, 1999. The report stated that the Defense Logistics Agency had taken many positive actions to address the Y2K problem. Some of the positive actions included prioritizing mission-critical systems, developing a Y2K Test and Evaluation Master Plan, and developing a contingency plan for the Distribution Standard System. However, there are several actions that the Defense Logistics Agency had not completed. Specifically, the Defense Logistics Agency did not:

- develop a depot-level checklist for consistent implementation of the Defense Logistics Agency Y2K Management Plan,
- ensure that interface agreements contained all necessary critical data,
- develop all required test plans or testing milestone schedules,
- ensure that the Distribution Standard System megacenter test domain was Y2K compliant, and
- ensure that test agreements between the Defense Megacenters and the Defense Logistics Agency, as required by Secretary of Defense policy, had been signed.

The report recommended that the Director, Defense Logistics Agency:

- develop and implement a depot-level Y2K checklist,
- complete the inventory of all Distribution Standard System interfaces and prepare interface agreements that contain the required data elements for all mission-critical interfaces,
- include the complete inventory of interfaces in the follow-on interface testing prior to Y2K certification, and
- develop a comprehensive test plan and schedule for the operational assessment and time machine testing.

The report also recommended that the Director, Defense Logistics Agency, in conjunction with the Director, Defense Information Systems Agency:

- ensure that the test domain is Y2K compliant prior to the certification of the Distribution Standard System as Y2K compliant,
- validate that the Y2K status reported for the Defense Megacenter domains is accurate and that the status of software attributed to each domain is accurate,

-
- obtain a waiver for the compiler associated with the Distribution Standard System test and production domains, and
 - initiate and sign explicit Distribution Standard System test agreements between the Defense Information Systems Agency megacenters and the Defense Logistics Agency as required by Secretary of Defense policy of August 7, 1998.

DLA stated that a depot-level checklist existed and the inventory of Distribution Standard System interfaces had been completed. DLA also stated that the DLA test and certification process requires test plans for the operational assessment and time machine testing and that a waiver had been granted allowing the use of the programming language compiler. Additionally, DLA stated that explicit test agreements had been signed with DISA. DLA nonconcurred with the recommendation to include the complete inventory of interfaces in the follow-on interface testing, stating that the Distribution Standard System is a compliant production system and that all interfaces were simulated during the validation testing. DLA also nonconcurred with the recommendation to ensure that the Distribution Standard System test domain was Y2K compliant prior to certification. DLA stated that it had a waiver that allows the Distribution Standard Systems Agency to be certified as compliant based on the existing testing. DISA concurred with the finding and all recommendations. In addition, DISA indicated that it would assist DLA in obtaining a waiver for the compiler and that explicit test agreements were in place for major customers. DLA completed its contingency plan for the Distribution Standard System and is refining the plan in preparation for the end-to-end testing. Action is ongoing.

Army Audit Agency

Memorandum Report No. AA99-353, “Audit of Mission Critical Weapon Systems – Year 2000 Assessment of the Standalone Airborne and the Cargo Utility Global Positioning System Receivers at the U.S. Army Communications-Electronics Command,” July 19, 1999. The memorandum stated that Department of the Army and the Product Manager took action to resolve six of the seven issues that were identified during the assessment. However, there are additional actions needed to mitigate one risk area. Specifically, command personnel needs to obtain contractor assurance regarding the Y2K compliance for nondevelopmental items supporting the two systems.

Memorandum Report No. AA99-352, “Audit of Mission Critical Weapon Systems – Year 2000 Assessment of the Firefinder Weapon Systems at the U.S. Army Communication – Electronics Command,” July 19, 1999. The memorandum stated that the Product Management Office personnel provided reasonable assurance supporting the Y2K compliance for the Firefinding Mortar Locating Radar (FF-Q36), Firefinder Artillery Locating Radar (FF-Q37), and the Firefinder Electronic Upgrade (FF-EU). There were six issues and risk areas requiring management attention. The Product Management Office personnel took action to resolve three of the issues and risk areas during the assessment. However, there are three issues and risk areas that remain open and require management attention.

The memorandum suggested that command personnel:

- review and approve the Y2K Certification Checklist for the FF-Q36, FF-Q37, and FF-EU;
- prepare a memorandum of understanding (or equivalent) between the Logistics Readiness Center and the Systems Management Center defining Y2K roles and responsibilities; and
- update the Army Y2K database to accurately reflect the current status of the FF-Q36, FF-Q37, and FF-EU.

The Product Manager was briefed and agreed with two of the three open issues. The Product Manager believed existing organizational roles and responsibilities have adequately addressed the third open issue.

Memorandum Report No. AA99-338, “Audit of Mission Critical Weapon Systems – Year 2000 (Phase VI); Assessment of the Medium Recovery Vehicle at the U.S. Army Tank-automotive and Armaments Command,” June 30, 1999. The memorandum stated that the Weapon System Management Office personnel provided reasonable assurance supporting Y2K compliance for the Medium Recovery Vehicle. However, the Army Audit Service identified some issues and risk areas requiring management attention.

The memorandum suggested that the Weapons Systems Manager for Heavy Tactical Vehicles:

- establish memorandums of agreements (or equivalent) with the component managers for common support items supporting the Medium Recovery Vehicle to ensure the items wouldn’t degrade operational capabilities for the weapon system. If component managers indicate that common support items have Y2K compliance issues, obtain contingency plans from the component managers to ensure users develop operational level workarounds;
- prepare, and have responsible parties sign a Y2K certification checklist for the Medium Recovery Vehicle; and
- update the Army’s Y2K database to accurately reflect the status of the Medium Recovery Vehicle.

Weapon Systems Management Office personnel and the Deputy Commander, U.S. Army Tank-automotive and Armaments Command were briefed. Command personnel generally agreed with the suggested actions, and agreed to implement them.

Memorandum Report No. AA99-337, “Audit of Mission Critical Weapon Systems – Year 2000 (Phase VI); Assessment of Medium Tactical Vehicles at the Office of the Program Executive Officer for Ground Combat and Support Systems,” June 29, 1999. The memorandum stated that the Project Management Office personnel provided reasonable assurance supporting Y2K

compliance for Medium Tactical Vehicles. However, during the assessment some issues requiring management attention were identified.

Project Management Office personnel responded to issues that were identified during the assessment. Specifically, the project office personnel:

- mitigated possible Y2K risks associated with the electronic control units by obtaining written assurance from the prime contractor on April 23, 1999, stating that the electronic control units residing on the Medium Tactical Vehicles are not impacted by the Y2K; and
- updated the Army's Y2K database to accurately reflect the status of Medium Tactical Vehicles.

As a result, no further action was required.

Memorandum Report No. AA99-336, "Audit of Mission Critical Weapon Systems – Year 2000 (Phase VI); Assessment of the Abrams Tank Systems at the Office of the Program Executive Officer for Ground Combat and Support Systems," June 29, 1999. The memorandum stated that Project Management Office personnel provided reasonable assurance supporting Y2K compliance for the Abrams Tank Systems. However, there were some issues and risk areas identified that required management attention. Project Management Office personnel have continually and aggressively addressed issues.

The memorandum suggested that the Project Manager for Abrams Tank Systems continue to track the Y2K compliance status for the contractors and government agencies supporting the Abrams program. If any of the contractors are publicly traded companies, project office personnel could access and monitor the contractor's Y2K compliance that is reported to the U.S. Securities and Exchange Commission.

The Project Management Office for Abrams Tank Systems and Program Executive Office for Ground Combat Support Systems both agreed with the suggested action.

Memorandum Report No. AA99-332, "Audit of Mission Critical Weapon Systems – Year 2000 (Phase VI); Assessment of High Mobility Multipurpose Wheeled Vehicle at the U.S. Army Tank-automotive and Armaments Command," June 29, 1999. The report states that Project Management Office personnel provided reasonable assurance supporting Y2K compliance for the High Mobility Multipurpose Wheeled Vehicle. However, some issue and risk areas requiring management attention were identified.

Project Management Office personnel addressed issues and mitigated risk areas that were identified in the assessment. However, additional actions were

needed to resolve current issues and risk areas. The memorandum suggested that the Project Manager for Light Tactical Vehicles.

- establish memorandums of agreement (or the equivalent) with the component managers for common support items supporting the High Mobility Multipurpose Wheeled Vehicle to ensure the items would not degrade operational capabilities for the weapon system. If component managers indicate that common support items have Y2K compliance issues, obtain contingency plans from component managers to ensure user develop operational level workarounds; and
- ensure the Y2K Compliance Checklist is approved in accordance with the Army's Y2K Action Plan.

Additionally, the memorandum suggested that the U.S. Army Materiel Command needed to review and approve the high Mobility Multipurpose Wheeled Vehicle Y2K Compliance Checklist.

The Project Management Office, U.S. Army Tank-automotive and Armaments Command and the Army Materiel Command generally agreed with the issues and our suggested actions.

Memorandum Report No. AA99-331, "Audit of Mission Critical Weapon Systems – Year 2000 (Phase VI); Assessment of Deployable Universal Combat Earthmover at the U.S. Army Tank-automotive and Armaments Command," June 29, 1999. The memorandum stated that Product Management Office personnel provided reasonable assurance supporting Y2K compliance for the Deployable Universal Combat Earthmover. However, some issues and risk areas requiring management attention were identified.

Product Management Office personnel have aggressively addressed issues and mitigated risk areas that were identified during the assessment, but additional actions are needed to resolve current issues and risk areas. The memorandum suggested that the Product Manager for Construction Equipment/Materials Handling:

- establish memorandums of agreement (or the equivalent) with the component managers for common support items used in the Deployable Universal Combat Earthmover to ensure the items won't degrade operational capabilities for the weapon system. If component managers indicate that common support items have Y2K compliance issues, the Product Manager needs to obtain contingency plans from component managers to ensure users develop operational level workaround;
- ensure the contract is modified to include the required Y2K contract language; and
- ensure the Y2K Compliance Checklist is approved in accordance with the Army's Y2K Action Plan.

Additionally, the memorandum suggested that the U.S. Material Command needed to review and approve the Deployable Universal Combat Earthmover Y2K Compliance Checklist.

Product Management Office, U.S. Army Tank-automotive and Armaments Command and the Army Materiel Command generally agreed with the identified issues, and agreed to implement the suggested actions.

Memorandum Report No. AA99-330, “Audit of Mission Critical Weapon Systems – Year 2000 (Phase VI); Assessment of Heavy Tactical Vehicles at the U.S. Army Tank-automotive and Armaments Command,” June 29, 1999. The memorandum stated that Program Management Office personnel provided reasonable assurance supporting Y2K compliance for the Palletized Load System, Heavy Equipment Transporter System, and Heavy Expanded Mobility Tactical Truck. However, there were some issue and risk areas that required management attention.

Program Management Office personnel have aggressively addressed the issues and risks areas that were identified in the assessment. However, there remains additional action that will resolve current issues and risk areas. The memorandum suggested that the Program Manager for Heavy Tactical Vehicles:

- establish memorandums of agreement (or the equivalent) with the component managers for the common support items supporting the Heavy Tactical Vehicles to ensure the items won't degrade operational capabilities for the weapon systems; and
- ensure all contracts are modified to include the required Y2K contract language.

Additionally, the memorandum suggested that the Commander, U.S. Army Tank-automotive and Armaments Command make sure that the Army's Y2K database is updated with complete and accurate information for the Palletized Load System, Heavy Equipment Transporter System, and Heavy Expanded Mobility Tactical Truck. The memorandum also suggested that the U.S. Army Material Command review and approve the Heavy Tactical Y2K Compliance Checklist.

The Program Management Office, U.S. Army Tank-automotive and Armaments Command and the Army Materiel Command generally agreed with identified issues and agreed to implement the suggested actions.

Memorandum Report No. AA99-290, “Audit of Mission Critical Weapon Systems – Year 2000 (Phase VI); Assessment of the Bradley Fighting Vehicle Systems at the Office of the Program Executive Officer for Ground Combat and Support Systems,” June 16, 1999. The memorandum stated that Project Management Office personnel provided reasonable assurance supporting Y2K compliance for the Bradley Fighting Vehicle Systems. During the assessment some issues requiring management attention for four of the nine Bradley systems – M2/M3AO, M2A1/M3A1, M2A2/M3A2 Operation Desert Storm, and the M6 Linebacker were identified.

In response to the issues that were identified in the assessment, the Bradley Fighting Vehicle Systems, Project Management Office personnel continually and aggressively addressed issues and mitigated risk areas. However, there are additional actions needed to resolve issues and risk areas. The memorandum suggested that the Program Executive Officer and Project Manager:

- Closely track, and maintain continual dialogue with responsible Project Management Office personnel to ensure all noncompliant Handheld Terminal Units are replaced in a timely and efficient manner prior to the millennium rollover.
- Ensure that the primary contract is modified to include the required Y2K language.
- Incorporate and Project Management Office changes and disseminate system contingency plans to users for ensuring operational workarounds are identified for the M2A2/M3A2 Operation Desert Storm and the M6 Bradley Linebacker.

The Project Management Office for Bradley Fighting Vehicle Systems and the Program Executive Office for Ground Combat and Support Systems both agreed with the suggested actions.

Memorandum Report No. AA99-283, "Audit of Mission Critical Weapon Systems – Year 2000 (Phase VI); Assessment of the Hercules Recovery Vehicle (M88A2) at the U.S. Army Tank-automotive and Armament Command," June 16, 1999. The memorandum stated that Product Management Office personnel provided reasonable assurance supporting Y2K compliance for the Hercules Recovery Vehicle. However, some issues and risk areas required were identified the management attention.

In response to the issue and risk areas identified, Product Management Office personnel took action to ensure diligence in supporting the Y2K compliance for the Hercules. However, additional actions were needed. The memorandum suggested that the Program Manager for Hercules:

- monitor the contractor's Y2K compliance status reported to the U.S. Securities and Exchange Commission. The contractor reported possible disruption to internal operations, which could conceivably disrupt U.S. Army operations and support for the Hercules. Therefore, Product Management Office personnel should access the U.S. Securities and Exchange Commission's web site for tracking the contractor's Y2K compliance status;
- establish Memorandums of Agreement (or equivalent) with the component managers for common support items supporting the Hercules Recovery Vehicle to ensure the items wouldn't degrade operational capabilities for the weapon system. If component managers indicate that common support items have Y2K compliance issues, obtain contingency plans from the component managers to ensure users have workarounds; and

-
- complete a separate Y2K Certification Checklist for the Hercules Recovery Vehicle (M88A2).

Additionally, the memorandum suggested that the Commander, U.S. Army Tank-automotive and Armaments Command, make sure that the Army's Y2K database is updated with accurate information regarding the Hercules Recovery Vehicle. Also, the U.S. Army Materiel Command needed to review and approve the Hercules Recovery Vehicle Y2K Certification Checklists.

The Product Management Office personnel and the Deputy Commander for the U.S. Army Tank-automotive and Armaments Command both agreed to monitor the contractor's Y2K readiness and establish memorandums of agreement with component managers. The Army Materiel Command changed the procedure for signing Y2K checklists. As of May 21, 1999, Major Subordinate Commands were authorized to sign the checklists.

Memorandum Report No. AA99-282, "Audit of Mission Critical Weapon Systems – Year 2000 (Phase VI); Assessment of the Paladin Self-Propelled Howitzer (M109A6) at the U.S. Army Tank-automotive and Armaments Commands," June 29, 1999. The memorandum stated that Product Management Office personnel provided only limited assurance supporting Y2K compliance for the Paladin Self-Propelled Howitzer (M109A6). Product Management Office personnel reported the Paladin as Y2K compliant; however documentation supporting compliance for the Paladin was not sufficiently provided. Specifically, Product Management Office personnel:

- did not have adequate documentation supporting Y2K testing for the Paladin; and
- have not tested the Paladin for Y2K compliance with its interfacing systems.

Based on the issues and risk areas that were identified during the assessment, Product Management Office personnel have taken action. However, additional actions were needed to resolve other issues and risk areas. The memorandum suggested that the Product Manager:

- document test plans, procedures, and results for the Paladin's system-level test to support Y2K compliance for the system;
- ensure the Paladin is tested for Y2K compliance with its interfacing systems and update U.S. Army Tank-automotive and Armaments Command and Army on the results of the interfacing testing;
- prepare and sign a new Y2K certification checklist for the Paladin based on the results of "system" and "interfacing systems" testing; and
- establish Memorandums of Agreement (or equivalent) with the component managers for common support items supporting the Paladin to ensure the items will not degrade operational capabilities

for the weapon system. If component managers indicate that common support items have Y2K compliance issues, obtain contingency plan from the component managers to ensure users have workarounds.

Additionally, the Commander, U.S. Army Tank-automotive and Armament Command, needs to make sure the Army's Y2K database is updated with complete and accurate information regarding the Paladin Self-Propelled Howitzer.

Product Management Office personnel and the Deputy Commander for the Army Tank-automotive Armaments Command generally agreed with the issues and agreed to implement the suggested actions.

Memorandum Report No. AA 99-238, "Audit of Mission Critical Weapon Systems –Year 2000 (Phase VI); Assessment of the Joint Tactical Ground Station at the Office of the Program Executive Officer for Air and Missile Defense," April 30, 1999. The memorandum stated that Project Management Office personnel exercised diligence and provided reasonable assurance supporting Y2K compliance for the Joint Tactical Ground Station. The Joint Tactical Ground Station is a key part of Commander in Chief Space Command's tactical event system operated by joint Army-Navy crews and provides continuous all weather threat monitoring.

There were some risk areas detected during the assessment that required management attention. These issues include: the Joint Tactical Ground Station is not currently scheduled for inclusion in any of the commander in chief's operational evaluations and the Project Management Office has not disseminated contingency plans for the Joint Tactical Ground Station to the users at the Space Command.

Suggested actions include requiring the Program Executive Officer and Project Manager to disseminate the Joint Tactical Ground Station contingency plan to the Space Command users. In addition, the report suggest, that the Director, Joint Staff, consider including the Joint Tactical Ground Station in a Joint Staff directed operation evaluation test to ensure interoperability and continuity of military operations.

Responsible personnel from the Project Manager Officer for Joint Tactical Ground Station and the Program Executive Office for Air and Missile Defense agreed with the suggested actions.

Memorandum Report No. AA 99-236, "Audit of Mission Critical Systems – Year 2000 (Phase VI); Assessment of the Chinook Cargo Helicopter (CH-47D) at the Office of the Program Executive Office for Aviation," April 14, 1999. The memorandum stated that the Chinook Cargo Helicopter's (CH-47D) operational capability would not be degraded by the Y2K rollover. The memorandum identified several risk areas, which the Project Management Office personnel took action. Some issues that were resolved included developing a risk management plan and preparing and signing interface

agreements. The suggested actions require the Program Executive Officer for Aviation and the Project Manager for Cargo Helicopters to:

- determine the status for the three outstanding interface agreements and ensure both parties come to closure with the terms in the agreements, and
- update the Army's Y2K database to accurately reflect the status of the Chinook Cargo Helicopter (CH-47D).

Memorandum Report No. AA 99-211, "Audit Mission Critical Systems – Year 2000 (Phase V); Assessment of the Blackhawk (UH-60A/L/Q) and Huey (UH-1) Utility Helicopters at the U.S. Army Aviation and Missile Command," March 30, 1999. The memorandum stated that Project Management Office personnel took a positive approach toward ensuring the Y2K compliance of the Blackhawk (UH-60A/L) and the Huey (UH-1) Utility Helicopters. However, some areas requiring management attention include: the digitized Blackhawk (UH-60Q) MEDEVAC, which processes dates, was not reported to the Army's Y2K database; the Y2K Certification Checklist was not adequately reviewed and approved; the Army Y2K database did not accurately reflect the Blackhawk (UH-60Q) MEDEVAC and the Blackhawk (UH-60A/L); and during compliance testing, the Program Management Office and contractor personnel encountered some Y2K leap year issues with the Control Display Units and the ARC-164 communications.

Suggested actions include the Commander, Army Aviation and Missile Command, and the Project Manager to:

- update the Army's Y2K database to accurately reflect the status of the Utility Helicopters to include the Blackhawk (UH-60Q) MEDEVAC and all interfacing systems with the Blackhawk and Huey, and
- resolve risk areas identified by contractors for the Blackhawk (UH-60Q) to ensure Y2K compliance, and monitor the Y2K, compliance testing scheduled for May 1999.

In addition, this report suggests that the Commander, Army Materiel Command, establish policy with the Assistant Secretary of the Army (Acquisition, Logistics and Technology) pertaining to roles, responsibilities, and procedures for reviewing and approving the weapon system Y2K Certification Checklist.

The Project Manager for Utility Helicopter and the Chief of Staff, Army Aviation and Missile Command, agreed with the suggested actions.

Memorandum Report No. AA 99-210, "Audit of Mission Critical Systems – Year 2000 (Phase V); Assessment of the Dragon at the U.S. Army Aviation and Missile Command," March 30 1999. The memorandum stated that the Weapons Systems Directorate personnel provided reasonable assurance supporting Y2K compliance for the Dragon Missile System. However, there was no interface agreement between the Weapon System Directorate for the

Dragon and the Project Manager for Test, Maintenance, and Diagnostic Equipment for the Intermediate Family of Test Equipment. Also, the Y2K Certification Checklist for the Dragon was not reviewed and approved by responsible personnel within the Army Material Command and Headquarters, the functional/system proponents. The status of the Dragon Missile System was not accurately reflected in the Army's Y2K database.

The memorandum suggested that the Commander, Army Aviation and Missile Command, and the Weapon System Directorate Manager:

- develop and sign an organizational interface agreement with the Project Manager for Test, Maintenance, and Diagnostic Equipment for the intermediate Family of Test Equipment identifying Y2K roles and responsibilities, and
- update the Army's Y2K database to accurately reflect the status of the Dragon.

Additional actions include requiring the Commander, Army Material Command, to establish policy with the Assistant Secretary of the Army (Acquisition, Logistics and Technology) pertaining to roles, responsibilities, and procedures for reviewing and approving weapon system Y2K Certification Checklist.

The Weapons Systems Directorate personnel and the Chief of Staff, Army Aviation and Missile Command, agreed with the recommendations.

Memorandum Report No. AA 99-209, "Audit of Mission Critical System – Year 2000 (Phase V); Assessment of Fixed Wing Aircraft at the U.S. Army Aviation and Missile Command," March 30, 1999. The memorandum stated that Product Management Office personnel exercised due diligence and provided reasonable assurance supporting Y2K compliance for the Gulfstream (C-20) and the Guardrail (RC-12) aircraft. However, the report provides some risk areas that require management attention. There was no memorandum of agreement, or updated maintenance agreement in place between the Product Manager for Fixed Wing and the Air Force establishing and identifying Y2K roles and responsibilities. Responsible personnel within the Army Material Command and Headquarters, the functional/systems proponents, have not reviewed and approved the Y2K Certification Checklist. Finally, the status of the Gulfstream (C-20) and the Guardrail (RC-12) was not accurately reflected in the Y2K database.

Suggested Actions for the Commander, Army Aviation and Missile Command, and the Product Manager to reduce risk of Y2K disruption include:

- developing and having both parties sign a memorandum of agreement, or modify the existing maintenance agreements, identifying Y2K roles and responsibilities for the fixed wing aircraft used by the U.S. Army, but maintained by the Air Force; and
- updating the Army Y2K database to accurately reflect the Gulfstream (C-20) and the Guardrail (RC-12).

The report also suggested that the Commander, Army Material Command, establish policy with the Assistant Secretary of Army (Acquisition, Logistics, and Technology) for reviewing and approving weapon system Y2K Certification Checklist.

Product Management Office personnel and the Chief of Staff, Army Aviation and Missile Command, agreed with the suggested actions. The Gulfstream (C-20) was tested on August 17, 1998, at Andrews Air Force Base, Maryland, and the Guardrail (RC-12) was tested on August 20, 1998, at Fort Belvoir, Virginia.

Memorandum Report No. AA99-208, "Audit of Mission Critical Systems – Year 2000 (Phase V); Assessment of the Short Range Air Defense Systems at the U.S. Army Aviation and Missile Command," March 30, 1999. The memorandum stated that the Project Management Office personnel provided reasonable assurance supporting the Y2K compliance of the Stinger Missile System, Stinger Field Handling Trainer, and Avenger Short-Range Air Defense System. However, there were no interface agreements in place between the Project Manager, Short-Range Air Defense Systems and the Army Simulation Training and Instrumentation Command for three trainers supporting the Stinger missile. The status of the Short-Range Air Defense System was not accurately reflected in the Army Y2K database. The assessment for the Stinger missile system did not include all platforms or identify subsystems the Marine Corps used. In addition, responsible personnel within the Army Material Command and the Army functional/system proponents have not reviewed and approved the Y2K Certification Checklist.

The report suggested that the Commander, Army Aviation and Missile Command, and the Project Manager:

- develop and have the Project Manager, Short-Range Air Defense Systems, and the Army Simulation Training and Instrumentation Command sign interface agreements for the three trainers supporting the Stinger missile;
- reassess the Stinger's platform for possible Y2K risks;
- update Project Management Office, Short-Range Air Defense System assessment matrices to accurately reflect systems the Project Management Office is responsible for; and
- update the Army's Y2K database to accurately reflect the status of the Short-Range Air Defense Systems.

In addition, the Commander, Army Material Command, is required to establish policy with Assistant Secretary of the Army (Acquisition, Logistics, and Technology) pertaining to roles, responsibilities, and procedures for reviewing and approving weapon system Y2K Certification Checklists.

Responsible personnel from the Project Management Office and the Chief of Staff, Army Aviation and Missile Command, agreed with the suggested actions.

Memorandum Report No. AA99-207, "Audit of Mission Critical Systems – Year 2000 (Phase V); Assessment of Scout Attack Weapon Systems at the U.S. Army Aviation and Missile Command," March 30, 1999. The memorandum stated that the Product Management Office personnel provided reasonable assurance supporting Y2K compliance for the Cobra (AH-1), Kiowa Scout (OH-58A/C), and the Kiowa Warrior (OH-58D) helicopters. However, some risk areas that required management attention include:

- system interface agreements between the Product Manager, Scout Attack and the Project Manager, Close Combat Anti-Armor Weapon System for the Tube Launched Optically Tracked Wire (TOW) guided missile,
- contracts did not include the mandatory Y2K contract language,
- Y2K Certification Checklist had not been reviewed and approved, and
- inaccurate database reporting.

The memorandum suggested that the Commander, Army Aviation and Missile Command, and the Product Manager:

- develop and have the Product Manager, Scout Attack and the Project Manager, Close Combat Anti-Armor Weapon System sign an interface agreement for the TOW;
- modify the contracts supporting the Kiowa Warrior to include the mandatory Y2K contract language; and
- update the Army's Y2K database to accurately reflect the status of the Cobra (AH-1), Kiowa Scout (OH-58A/C), and the Kiowa Warrior (OH-58D).

Additional actions include requiring the Commander, Army Materiel Command, to establish policy with the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) pertaining to roles, responsibilities, and procedures for reviewing and approving weapon system Y2K Certification Checklists.

The Product Manager for Scout Attack and the Chief of Staff, Army Aviation and Missile Command, agreed with the suggested actions.

Memorandum Report No. AA99-206, "Audit of Mission Critical Weapon System – Year 2000 (Phase V); Assessment of the Javelin Missile System at the Office of the Program Executive Officer for Tactical Missiles," March 31, 1999. The memorandum stated that the Project Management Office personnel exercised due diligence and provided reasonable assurance supporting Y2K compliance for the Javelin Missile System. However, there were some risk areas that required management attention including contracts, Y2K certification checklist, and database reporting. There was no assurance that the contractor's software development/ maintenance environments are Y2K

compliant. Six contracts supporting the Javelin Missile System did not have the required Y2K contract language. The Checklist for the Javelin Missile System was not reviewed and approved by the Army, functional/system proponent. In addition, the status of the Javelin Missile System was not accurately reflected in the Army's Y2K database.

The memorandum did provide recommendations for the Program Executive Officer and Project Manager to:

- obtain written assurance from the contractor that software development and maintenance environments are Y2K compliant,
- modify the six existing contracts with information technology deliverables to include Y2K related Federal-acquisition regulation language, and
- update the Army Y2K database to reflect the accurate status of the Javelin Missile System.

The Project Management Office for Javelin and the Program Executive Office for Tactical Missiles agreed with the suggested actions.

Memorandum Report No. AA99-205, "Audit Mission Critical Systems – Year 2000 (Phase V); Assessment of the Army Tactical Missile System at the Office of the Program Executive Officer for Tactical Missile," March 31, 1999. The memorandum stated that the Project Management Office personnel exercised due diligence and provided reasonable assurance supporting Y2K compliance for the Army Tactical Missile System. However, there were some risk areas that require management attention. A systems assessment and certification for 100 percent of the hardware, software, and devices wasn't completed prior, or during the Y2K assessment. The Y2K Certification Checklist for the Army Tactical Missile System was not reviewed and approved by the Army functional/system proponents. In addition, the Army's Y2K database didn't accurately reflect the status of the Army Tactical Missile System.

The memorandum suggested that the Program Executive Officer and Project Manager:

- complete the assessment of system hardware, software, and devices, and
- update the Army Y2K database to reflect the accurate status of the Army Tactical Missile System.

The Project Manager Office for the Army Tactical Missile System and the Program Executive Office for Tactical Missile agreed with the suggestions. Responsible personnel successfully demonstrated Y2K compliance for the Army Tactical Missile System and some of its mission-critical interfacing systems during a live-fire test at the White Sands Missile Range in White Sands, New Mexico, on September 17, 1998.

Memorandum Report No. AA99-204, “Audit of Mission Critical Systems – Year 2000 (Phase V); Assessment of the Air-to-Ground Missile Systems at the Office of the Program Executive Office for Tactical Missiles,” March 31, 1999. The memorandum stated that the Project Management Office provided reasonable assurance supporting Y2K compliance for mission-critical air-to-ground missile systems. However, several risk areas remain that require management attention. One contract supporting the Hellfire II missile didn’t include the mandatory Y2K contract language. Interface agreements were not in place between Air-to-Ground Missile Systems and the Cobra. Also, the Y2K checklist was not reviewed and approved by the Army functional/system proponent. The status of Air-to-Ground Missile Systems was not accurately reflected in the Army’s Y2K database.

The memorandum recommended the Program Executive Officer and the Project Manager to:

- modify the one existing contract with the Y2K deliverables to include Y2K related Federal acquisition regulation language,
- develop and have all parties sign system interface agreements and memorandums of agreement for all interfacing systems, and
- update the Army Y2K database to reflect the accurate status of the Air-to-Ground Missile Systems.

The Project Manager for Air-to-Ground Missile Systems and the Program Executive Office personnel from Tactical Missiles agreed with the suggested actions. In addition, responsible personnel have demonstrated Y2K compliance for the Air-to-Ground Missile Systems during a live fire-test on November 24, 1998, at the White Sands Missile Range, New Mexico.

Memorandum Report No. AA99-203, “Audit of Mission Critical Weapon Systems – Year 2000 (Phase V); Assessment of the Multiple Launch Rocket System at the Office of the Program Executive Officer for Tactical Missiles,” March 31, 1999. The memorandum stated that Project Office personnel exercised due diligence and provided reasonable assurance supporting Y2K compliance for the Multiple Launch Rocket System. However, there were some risk areas that required management attention. A systems assessment and certification for 100 percent of the hardware, software, and devices wasn’t completed prior to, or during the Y2K assessment. Two contracts supporting the Multiple Launch Rocket System did not have the required Y2K contract language. In addition, the status of the Multiple Launch Rocket was not accurately reflected in the Army’s Y2K database.

The memorandum suggested the Program Executive Officer and Project Manager to:

- complete the assessment of the system hardware, software, and devices,

-
- modify the two existing contracts with information technology deliverables to include Y2K related Federal acquisition regulation language, and
 - update the Army Y2K database to reflect the accurate status of the Multiple Launch Rocket System.

The Project Management Office for Multiple Launch Rocket System and the Program Executive Office for Tactical Missiles agreed with the suggested actions and are taking action.

Memorandum Report No. AA99-202, "Audit of Mission Critical Weapon Systems – Year 2000 (Phase V); Assessment of Close Combat Anti-Armor Weapon Systems at the Office of the Pentagon Executive Officer for Tactical Missiles," March 31, 1999. The report stated that Project Manager Office personnel exercised due diligence and provided reasonable assurance supporting Y2K compliance for the Close Combat Anti-Armor Weapon Systems, including the Improved Target Acquisition System Improved Bradley Acquisition System, TOW Guided Missile, and the Bradley Fighting Vehicles-TOW-2 Subsystem. However, there were some risk areas that required management attention:

- there was no system interface agreement in place between the Army's TOW Guided Missile and the Navy's Super Cobra Helicopter (AH-1).
- there was no interoperability testing planned or scheduled for Y2K compliance between the TOW Missile and the Navy's Super Cobra Helicopter (AH-1).
- Army functional/systems proponents haven't reviewed and approved Y2K Certification Checklists for the Improved Bradley Acquisition System and the Bradley Fighting Vehicles System-TOW-2 Subsystem.

The memorandum suggested that the Program Executive Officer and Project Manager:

- develop and have all parties sign system interface agreements and memorandums of agreement between the TOW Guided Missile and the Navy's Super Cobra Helicopter (AH-1), and
- update the Army, Y2K database to reflect the accurate status of the Improved Bradley Acquisition System, TOW Guided Missile, and the Bradley Fighting Vehicle Systems-TOW-2 Subsystem.

Additional suggested actions include requiring the Navy Chief Information Officer, to include the Navy's AH-1 Super Cobra helicopter and the TOW Guided Missile in a test to ensure interoperability and continuity of military operations.

The Project Manager Office for Close Combat Anti-Armor Weapon System and Program Executive Office for Tactical Missile agreed with the suggested actions.

Naval Audit Service

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Marine Corps Air Station (MCAS) Cherry Point, North Carolina – July 14, 1999. The report stated that the Naval Audit Service considers MCAS Infrastructure to be in the Implementation Phase, with approximately 88 percent of infrastructure completed. MCAS Cherry Point did not meet the DoD and Navy Y2K target completion dates for its Shore Infrastructure Systems, Devices, and Infrastructure. The MCAS was certified Y2K compliant in March 15, 1999, with two significant infrastructure expectations. However, the Naval Audit Service believes that MCAS has identified and is managing all potential Y2K vulnerabilities.

The Naval Audit Service recommended that:

- MCAS monitor progress of the two Infrastructure systems Precision Measuring Equipment and Emergency Management Control System behind schedule and forward revised status of each to Naval Audit Service.
- MCAS continue to track the status of those system used by MCAS that require Y2K certification by other DoD activities and report the status of these systems to the Naval Audit Service.
- MCAS obtain Y2K status and certification from Naval Air Systems Command for the six station aircraft and provide documentation of this action, which should be completed by July 31, 1999, to the Naval Audit Service.
- MCAS should evaluate the need to apply addition resources to accelerate facilities Y2K compliance.

MCAS should finalize COOP documentation and report the status to the Naval Audit Service by July 31, 1999.

Memorandum: "Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy," Marine Corps Base (MCB), Camp Pendleton (CPEN), California – July 1, 1999. The report stated that Naval Audit Service considers Marine Corps Base, Camp Pendleton to be in the implementation phase for its Shore Infrastructure Systems, Devices, and Infrastructure, which did not meet the DoD and the Navy's Y2K target completion dates. Marine Corps Base, Camp Pendleton expected to complete its Shore Infrastructure Systems, Devices, and Infrastructure by August 31, 1999. Marine Corps Base, Camp Pendleton is in the process of completing its COOP. However, the draft contingency plans were reviewed and found to be adequate. Contingency plans and COOP are scheduled to be exercised be August 31, 1999.

The report recommended that Marine Corps Base, Camp Pendleton:

- complete the COOP and submit it to Headquarters, Marine Corps and provide the Naval Audit Service with an updated status on the COOP by July 31, 1999, and monthly updates afterward;
- determine, in conjunction with Marine Chief Information Officer, if memorandums of agreement and interfaces are needed and advise the Naval Audit Service of actions taken on July 31, 1999 and at the end of each month thereafter until actions have been completed on memorandums of agreement and interfaces;
- provide additional resources, as feasible, to expedite the completion of systems remaining to be replaced and provide the Naval Audit Service with an updated status on these systems on July 31, 1999, and monthly afterward until all systems are completed; and
- complete the testing of devices and provide the Naval Audit Service with an updated status of the testing on July 31, 1999, and monthly afterward until all testing is completed.
- complete the reviews of the 86 software packages. Provide the Naval Audit Service with an update on the review on July 31, 1999, and monthly afterward until all review is completed.

Memorandum: “Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy,” Military Sealift Command – June 17, 1999. The memorandum states that the Naval Audit Service considers the Military Sealift Command (MSC) to be in the implementation phase for its mission support systems and its Shore infrastructure systems, devices, and infrastructure, which includes all systems (mission critical and mission support) on its ships. The Naval Audit Service believes that MSC must continue its current level of effort to complete implementation in November as scheduled.

The Naval Audit Service recommended that the MSC update the Navy Y2K Tracking System and request the Navy Chief Information Officer to assist MSC editors to update those data elements that MSC cannot modify. In addition, MSC should develop a plan of action and milestones for completing implementation of both infrastructure categories and report the status to Naval Audit Service by July 31, 1999.

Memorandum: “Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy,” Naval Air Warfare Center, Weapons Division – June 11, 1999. The report states that the Naval Audit Service considers Naval Air Warfare Center, Weapons Division (NAWCWD) to be in the implementation phase for the Navy Y2K Tracking Systems mission support systems although it has three local systems in the renovation phase. NAWCWD did not meet the DoD and Navy Y2K target completion dates for its mission support systems, and Information Technology Infrastructure and Devices.

The Naval Audit Service recommended that:

- The Program Manager should ensure that a NAWCWD COOP is prepared and completed, operational, and tested.
- NAWCWD should provide additional resources, as feasible, to expedite the completion of systems remaining in the Renovation Phase
- NAWCWD should provide additional resources, as feasible, to expedite the completion of the Intrusion Detection System.
- The Navy Chief Information Officer and Commander in Chief, Pacific Fleet, should ensure that transfer the Automated Billing System is completed as soon as possible.
- NAWCWD should review/test Commander in Chief, Pacific Fleet, Contingency Plans for the Base Automated Billing System and the Targets Inventory and Performance Database to ensure reliability and coverage.
- NAWCWD should report the results of the testing of the 100 users within their network to Naval Audit Service by June 30, 1999 and each month thereafter until the personal computer testing is completed.

The memorandum stated that NAWCWD reports 155 of their 165 mission support line items are complete.

Memorandum: “Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy,” The Naval Sea System (NAVSEA) Command, Smart Ship Program and Smart Gator Offices – May 27, 1999. The memorandum states that the Naval Audit Service considers NAVSEA Smart Ship Program and Smart Gator Project to be in the completed phase for mission-critical systems and in the implementation phase for mission-support systems. Based on the results of the review, NAVSEA Smart Ship and Smart Gator met the DoD and Navy Y2K target completion dates for mission-critical systems and did not meet the target completion dates for mission-support systems. The Smart Ship Program and the Smart Gator Project Office did not have proper documentation available to support the independent tests or audits conducted that were necessary to achieve the level one or two certification.

The memorandum recommended that:

- NAVSEA should reconcile all 25 vulnerable systems and correctly update the Navy Y2K Tracking System.
- NAVSEA should determine whether the fiber optic local area networks should be reported as a system or as Infrastructure.

-
- NAVSEA should obtain signed documentation from the tester or auditor detailing their level of independence and the methodology used to perform the test or audit. Additionally, describe the test environment and test results.
 - NAVSEA should devote additional resources where applicable to expedite implementation.

The memorandum stated that the NAVSEA Smart Ship Program Office is internally tracking and reporting 12 systems (3 mission-critical and 9 support systems) as complete and that the NAVSEA Smart Gator Project Office is internally tracking and reporting 7 systems (2 mission-critical and 5 mission support systems) as complete.

Memorandum: “Review of the Year 2000 (Y2K) Processing Problem in the Department of the Navy,” The Puget Sound Naval Shipyard – May 18, 1999. The memorandum stated that the Naval Audit Service considers the Puget Sound Naval Shipyard to be in the implementation phase for Shore Infrastructure Systems, Devices, and Infrastructure; and to be in the renovation phase for its 27 mission support NAVSEA corporate systems. Three of the NAVSEA’s 27 corporate systems remain in the renovation phase. In addition, the Puget Sound Naval Shipyard had not updated its continuity of operations plans for possible Y2K failures and developed a contingency plan for corporate systems and infrastructure having high impact on shipyard operations.

The memorandum recommended that the Puget Sound Naval Shipyard:

- develop continuity of operation plans for the two core mission functions not covered,
- obtain (and continue to track) Y2K status for all infrastructure devices and equipment associated with critical operations,
- develop, document and test realistic contingency plans for the mission support corporate NAVSEA systems still in renovation, and
- perform Y2K testing as the hardware is received and configured with software prior to distribution throughout the shipyard.

Memorandum: “Review of the Year 2000 (Y2K) Processing Problem in the Department of the Navy,” The Naval Air Warfare Center, Aircraft Division, Patuxent River, Maryland, May 12, 1999. The memorandum stated that the Naval Audit Service considers the Naval Air Warfare Center, Aircraft Division, to be in the validation phase for the Naval Y2K Tracking System mission support systems although eight systems are in the renovation phase. The Shore Infrastructure Systems, Devices, and Infrastructure were completed. The Information Technology Shore Infrastructure Systems, Devices, Infrastructure is in the inventory phase. Consequently, the Naval Air Warfare Center, Aircraft Division, will not meet the DoD and Navy’s Y2K target completion dates for its mission support systems, and Information Technology Infrastructure and Devices.

The memorandum made recommendations for the Naval Air Warfare Center, Aircraft Division, to:

- develop plans to conduct a physical inventory of the Information Technology Infrastructure and Devices,
- ensure a Naval Air Warfare Center, Aircraft Division, Continuity of Operation Plan is prepared and operational,
- provide additional resources to expedite the renovation phase completion for the systems behind schedule,
- provide copies of completed contingency plans for those system that were not completed by March 31, 1999, to the Navy Chief Information Officer Office by June 14, 1999,
- require the independent contractors to ensure all DoD and Navy Y2K test requirements are performed, validated and documented prior to issuing the certification recommendation,
- develop test plans, establish test dates, and document test results of established interfaces for certified systems, and
- correct erroneous strategy fields within the Navy Y2K Tracking System for their systems.

Memorandum: "Review of the Year 2000 (Y2K) Processing Problem in the Department of the Navy," Marine Corps Systems Command, April 23, 1999. The memorandum stated that the Naval Audit Service considers the Marine Corps Systems Command to be in the implementation phase for its mission-critical systems, mission support systems, Shore Infrastructure Systems, Devices, and infrastructure. The Naval Audit Service believes that the Marine Corps Systems Command will not meet the DoD and Navy Y2K target completion dates for the mission-critical systems. Based on the results of the Navy's review of infrastructure, the Marine Corps Systems Command will not meet the DoD and Navy target completion dates. The Marine Corps Systems Command is in the process of certifying all systems at level 2.

Although the Marine Corps Systems Command is taking positive actions addressing its Y2K problems, the memorandum offered several recommendations for the Marine Corps Systems Command, to:

- prepare a Continuity of Operations Plan,
- ensure that the Fitness Report Optical Digital Imaging Systems and Automated Claims Information System are correctly reported to the Naval Y2K Tracking System to include the proper Y2K strategy and ensure reporting of any replacement system if applicable,
- accelerate the completion of Mission Critical and Mission Support line items as appropriate,

-
- ensure status is communicated to Senior manager and current status correctly reflected in the Naval Y2K Tracking Systems,
 - ensure that the new development system have contingency plans in place before deployment, and

Memorandum: “Review of the Year 2000 (Y2K) Processing Problem in the Department of the Navy,” The Chief of Naval Personnel, April 23, 1999.

The memorandum stated that the Naval Audit Service considers the Naval Personnel Command to be in the renovation phase for the Naval Y2K Tracking System Program of Record mission-critical and mission-support systems, and the implementation phase for its Shore Infrastructure Systems, Devices, and Infrastructure. Specifically, the Chief of Naval Personnel did not meet the DoD and Navy’s Y2K target completion dates for mission-critical program of record systems and will not meet the deadlines for mission-support program of record systems.

The memorandum provides several recommendations for the Chief of Naval Personnel, to:

- expedite the Renovation Phase completion of the systems behind target completion date for the renovation phase,
- expedite completion of the two mission critical and six mission support line items,
- request funding to certify all systems at Level 2 for Y2K compliance,
- request that the Operational Test & Evaluation Force certify systems as Y2K compliant,
- review the mission-critical coding of devices in the Naval Y2K tracking Systems to ensure that mission criticality is accurately reported, and
- expedite the assessment of the remaining infrastructure devices in the assessment phase.

Memorandum: “Review of the Year 2000 (Y2K) Processing Problem in the Department of the Navy,” Commander, Naval Reserve Forces, April 23, 1999.

The memorandum stated that the Naval Audit Service considers the Naval Reserve Forces’ systems to be in the validation phase; the facilities infrastructure to be in the implementation phase; and the Industrial and Information Technology infrastructure to be in the assessment phase. Mission-critical systems have not met the Navy’s Chief Information Officer implementation target date. Shore Infrastructure Systems, Devices and Infrastructure are unlikely to meet the DoD and the Navy’s March 31, 1999, target completion deadlines. Naval Audit Service also believes that the Commander, Naval Reserve Forces’ Systems and Infrastructure, will not meet the Navy’s Y2K target completion dates, but will be fully implemented prior to December 31, 1999.

The memorandum provides several recommendations for the Commander, Naval Reserve Forces, to:

- review and correct Navy Y2K Tracking Systems data to accurately reflect costs, replacement systems, systems status, interfaces, and MOAs;
- expedite the completion and testing of the Continuity of Operation Plan;
- track and obtain Y2K compliance of Defense Megacenter mainframes and operating systems that are used by the Reserve Financial Manager System;
- finalize the three draft contingency plans for mission-critical systems and develop contingency plans for two mission-critical systems Reserve Standard Training Administration and Readiness Support; and.
- track and ensure Y2K certification by external organizations for all ships, aircraft flight simulators and other such training devices impacting Commander, Naval Reserve Forces, mission and training.

Memorandum: “Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy,” Naval Facilities Engineering Command, April 22, 1999. The memorandum stated that the Naval Audits Service considers the Naval Facilities Engineering Command to be in the Renovation Phase for its Navy Y2K Tracking Systems, to be in the Implementation Phase for its Information Technology Infrastructure and Devices, and to be in the Assessment Phase for its Industrial Infrastructure and Devices. The Naval Audit Service believes that the Naval Facilities Engineering Command will meet the DoD and Navy target completion dates for IT Infrastructure and Devices.

However, the Naval Audit Service believes that the Naval Facilities Engineering Command will not meet the DoD and the Navy target date for the mission support systems and the Industrial and Facilities Infrastructure. Other areas of concern include: the estimated Y2K cost that the Naval Facilities Command reported to the Navy Y2K Tracking System for individual systems does not reflect updated cost; the Naval Facilities Engineering Command did not provide a Continuity of Operation Plan or submit comprehensive contingency plans for all of its mission-support systems; and only 5 of the 155 mission support systems were reported in the validation phase.

The memorandum provides several recommendations for the Naval Facilities Engineering Command to:

- update Y2K cost to reflect actual cost for the completed systems,
- develop a Continuity of Operations Plan in accordance with guidance in the Navy’s Chief Information Officer Y2K Action Plan,

-
- visit field sites to coordinate the Y2K activity and to ensure that the Continuity of Operations Plans are current and updated for Y2K issues,
 - develop contingency plans for those systems being renovated because of late delivery of replacement systems,
 - expedite completion of the mission-support systems and test contingency plans for all systems to ensure adequacy,
 - ensure the validation testing is performed for all systems per the Navy Chief Information Officer Y2K Action Plan, and
 - expedite completion of the mission-support systems in the validation phase and provide plan of action and milestones to Naval Audit Service.

Memorandum: “Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy,” Headquarters, Naval District Washington, March 2, 1999. The memorandum stated that the Naval Audit Service considers the Naval District Washington to be in the implementation phase for Shore Infrastructure Systems, Devices, and Infrastructure. The Naval Audit Service believes that the Naval District Washington will meet the DoD and Navy Y2K target date. However, the Naval District Washington has two mission-critical facilities items that are not compliant. In addition, approximately half of the devices identified as mission critical were improperly coded as mission critical and do not meet the Navy Chief Information Officer’s contingency plan requirements. The Naval District Washington is still in the process of developing its continuity of operation plans. Other areas of concern include the Naval District Washington’s major contract for information technology replacements did not disclose the appropriate Y2K language and the Naval District Washington did not identify major systems with established interfaces to ensure proper function.

The memorandum recommended that the Naval District Washington:

- devote additional resources for finalizing contingency plans for its mission critical infrastructure systems,
- devote additional resources for finalizing continuity-of-operation plans as required by Navy Chief Information Officer’s Y2K Action Plan,
- review all current contracts and leases to ensure that Y2K contract language is in accordance with Federal Acquisition Regulation 39.002 guidance,
- revisit its implementation schedule to ensure its two mission-critical facilities line items receive top priority, and

-
- identify all major system interfaces and ensure that the interfaces will work properly.

Memorandum: “Review of Year 2000 (Y2K) Processing Problem in the Department of the Navy,” Office of Naval Intelligence, February 10, 1999. The memorandum stated that the Naval Audit Services considers the Office of Naval Intelligence to be in the assessment phase, the second of three phases outlined in the September 1998 Navy Chief Information Officer’s Action Plan for Shore Infrastructure Systems, Devices, and Infrastructure. The Naval Audit Service believes that the Office of Naval Intelligence will not meet the Department of Defense and the Department of the Navy’s Y2K target completion dates. Specifically, the Office of Naval Information infrastructure reports to the DoD Chief Information Officer did not identify mission criticality, the continuity-of-operation plans were still being developed, and the Office of Naval Intelligence reported six information technology infrastructure (communication devices) as unknown Y2K status.

The memorandum recommended that the Office of Naval Intelligence:

- include infrastructure mission criticality in reports submitted to Navy’s Chief Information Officer,
- ensure applicable infrastructure devices, which could impact core mission functions, are incorporated in continuity-of-operation plans, and
- in conjunction with Naval District Washington, expedite the assessment of Y2K compliance for the remaining information technology infrastructure and productivity device infrastructure.

Air Force Audit Agency

Briefing Report, “Continuity of Mission and Support Function for the Year 2000 Program,” March – July 1999. The briefing report states overall, Air Force organizations effectively addressed functions essential for day-to-day mission continuity in regard to the Y2K issue. Specifically, installation senior leaders and Y2K program personnel generally applied diligence in addressing program criteria. However, of the 11 installations reviewed:

- The Air National Guard, Air Force Reserve Command, Air Force in Europe, and Pacific Air Forces did not effectively management inventory efforts.
- The Air National Guard and the Air Force in Europe did not effectively manage assessment efforts.
- The Air National Guard, Air Force Reserve Command, and the Pacific Air Forces did not effectively manage fix efforts.

-
- The Air National Guard, Air Force in Europe, and Pacific Air Forces did not effectively address Continuity of Operations Plan requirements.

The inventory efforts required that the inventory is complete with criticality properly assigned, installation and organization inventories are in agreement, equipment coordination is centrally managed, and risk analysis is effective. The assessment efforts required that the fix efforts are scheduled and planned, costs are identified through appropriate channels, and progress is sufficient. The fix efforts required that the contingency plans are prepared, consequence management teams are addressed, contingency plan development has the appropriate personnel involved, the contingency plan is approved at an appropriate level, and there is sufficient progress. The COOPs efforts require that the senior leader and other appropriate installation personnel be involved in COOPs preparation, COOP development efforts are documented, COOPs are approved at an appropriate level, COOP exercise actions are planned, and appropriate personnel are involved in COOP exercises. The briefing suggested that Air Force organizations:

- identify units with inventory shortfalls to squadron and group commanders to generate the necessary actions for finalizing inventory requirements;
- accomplish inventory walk-throughs to complete 100% inventories, with a focus on mission critical and mission essential functions;
- improve the overall timeliness of assessment efforts;
- accomplish follow-up action as necessary;
- increase senior-level attention to assure proper funding and timely fix action and prioritize remaining program actions according to assigned criticality levels;
- coordinate base-wide requirements to develop and complete contingency plans;
- incorporate consequence management teams into planning process;
- increase senior management involvement to ensure all appropriate personnel participate in the overall process; and
- development efforts are properly documented for continuity purposes.

Inspector General, Marine Corps

Marine Corps Air Station, Miramar, June 15-Jun 17, 1999. The Inspector General, Marine Corps, provided inspection results for the Marine Corps Air Station, Miramar. The results show that the Marine Corps has taken positive

actions to address Y2K issues. For example, system contingency plans have been developed and placed on the Y2K web site for review. In addition, a helpdesk will be manned during the time of the century rollover. There will be 24-hour full operational capabilities for facilities from December 31, 1999, through January 1, 2000, and also on all other designated critical dates. However, efforts are still ongoing to ensure full Y2K compliance including the 253 upgrades that are scheduled for current noncompliant computers. The remaining noncompliant computers are slated to be replaced.

Marine Corps Recruit Depot, San Diego, March 9-March 11, 1999. The inspection results show that the Marine Corps Recruit Depot, San Diego, has taken positive actions to address its Y2K related issues. It has developed a Y2K Management Plan that is modeled after the DoD Y2K Management Plan and is complete with progress milestones. Contingency plans have been developed for systems that are noncompliant and systems that are being renovated. In addition, plans are in place for Emergency Response Teams and an Emergency Operations Center has been created and is self sufficient for power and communications. Additional planning is ongoing for contingencies not addressed in this inspection but directly related to the mission of the Depot, including planning for the possibility of airline disruption in the movement of recruits to and from the depot for training, as well as providing food for delivery service. Noncompliant personal computers have been identified and were sent to the Defense Reutilization and Marketing Office for disposal.

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
Principal Deputy Under Secretary for Acquisition and Technology
Deputy Under Secretary of Defense (Environmental Security)
Deputy Under Secretary of Defense (Industrial Affairs and Installations)
Deputy Under Secretary of Defense (Logistics)
Director, Defense Procurement
Director, Defense Research and Engineering
Director, Defense Logistics Studies Information Exchange
Director, Strategic and Tactical Systems
Director, Test Systems Engineering and Evaluation
Assistant to the Secretary of Defense (Nuclear, Chemical, and Biological Defense Programs)
Under Secretary of Defense for Policy
Under Secretary of Defense (Comptroller)
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Director, Program Analysis and Evaluation
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Health Affairs)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Deputy Assistant Secretary of Defense (Command, Control, Communications, Intelligence, Surveillance, Reconnaissance, and Space Systems)
Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
Principal Director for Year 2000
Assistant Secretary of Defense (Legislative Affairs)
Director, Operational Test and Evaluation

Joint Staff

Director, Joint Staff

Department of the Army

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

Department of the Navy

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

Department of the Air Force

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

Unified Commands

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

Other Defense Organizations

Director, Ballistic Missile Defense Organization
Chief Information Officer, Ballistic Missile Defense Organization
Director, Defense Advanced Research Projects Agency
Chief Information Officer, Defense Advanced Research Projects Agency
Director, Defense Commissary Agency
Chief Information Officer, Defense Commissary Agency
Director, Defense Contract Audit Agency
Chief Information Officer, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Chief Information Officer, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Chief Information Officer, Defense Information Systems Agency
Inspector General, Defense Information Systems Agency
United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Legal Services Agency
Chief Information Officer, Defense Legal Services Agency

Other Defense Organizations (cont'd)

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

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
Office of Information and Regulatory Affairs
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 Defense, Committee on Appropriations
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology,
Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, International Relations,
Committee on Government Reform
House Subcommittee on Technology, Committee on Science

Audit Team Members

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

Thomas F. Gimble
Patricia A. Brannin
Mary Lu Ugone
James W. Hutchinson
Timothy J. Harris
John J. Jenkins
Maria R. Palladino
James S. Moon
Jamal E. Hall