Audit Report

NAVY LOGISTICS YEAR 2000 END-TO-END TEST PLANNING

Report No. D-2000-040 November 16, 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, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

CAIMS	Conventional Ammunition Integrated Management System
DLA	Defense Logistics Agency
DUSD(L&MR)	Deputy Under Secretary of Defense (Logistics and Materiel Readiness)
NAVSEA	Naval Sea Systems Command
NAVSUP	Naval Supply Systems Command
PSA	Principal Staff Assistant
SALTS	Streamlined Automated Logistics Transmission System
SPAWAR	Space and Naval Warfare Systems Command
UADPS	Uniform Automated Data Processing System
Y2K	Year 2000

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

November 16, 1999

MEMORANDUM FOR DEPUTY UNDER SECRETARY OF DEFENSE
(LOGISTICS AND MATERIEL READINESS)
INSPECTOR GENERAL, DEPARTMENT OF THE NAVY

SUBJECT: Audit Report on Navy Logistics Year 2000 End-to-End Test Planning (Report No. D-2000-040)

We are providing this report for review and comment.

DoD Directive 7650.3 requires that all recommendations be resolved promptly, and there is special urgency regarding year 2000 conversion issues. The Chief Information Officer, Department of the Navy, did not comment on a draft of this report; therefore, we request that the Chief Information Officer provide comments on the final report by December 16, 1999.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Tilghman Schraden at (703) 604-9186 (DSN 664-9186) (tschraden@dodig.osd.mil) or Ms. Mary E. Geiger at (703) 604-9615 (DSN 664-9615) (mgeiger@dodig.osd.mil). See Appendix D for the report distribution. Audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2000-040 **November 16, 1999**
(Project No. 9LD-9024.03)

Navy Logistics Year 2000 End-to-End Test Planning

Executive Summary

Introduction. This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge. For a complete listing of audit projects addressing the issue, see the year 2000 web pages on the IGnet at http://www.ignet.gov.

The DoD Year 2000 Management Plan (DoD Management Plan) assigns responsibility to the Principal Staff Assistants for ensuring the end-to-end functional process flows that support their functional area are assessed either in a Joint Staff or commander in chief year 2000 (Y2K) operational evaluation, a Service-sponsored system integration test, or a functional area Y2K end-to-end test. The Principal Staff Assistants are also responsible for planning, executing, and evaluating all mission-critical systems not otherwise tested and ensuring that processes that fall within their purview are evaluated. The Deputy Under Secretary of Defense (Logistics and Materiel Readiness) (DUSD[L&MR]) acts on behalf of the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Principal Staff Assistant for logistics, in performing those functions for the logistics functional area. Logistics end-to-end test planning was accomplished through the "Logistics Capstone Operational Assessment Plan for Year 2000" (Logistics Capstone Plan).

Logistics functional end-to-end testing was divided into three phases. Level I was intra-Component testing, and Level II was inter-Component testing. Level III testing was to be conducted as required to perform retesting. The DUSD(L&MR) provided oversight for Level II testing while delegating responsibility for execution of Level I testing to the Components. Level II testing began on May 25, 1999, and was completed on July 14, 1999. The final report for Level II testing, "Logistics Year 2000 End-to-End Level II Exercise Evaluation Report," October 1999, prepared by the independent evaluator, the Joint Interoperability Test Command, concluded that mission-critical logistics processes will continue unaffected by Y2K issues. DUSD(L&MR) representatives stated that Level III testing would not be required because of the successful demonstration of Y2K capabilities by the logistics systems participating in the test of the five critical core logistics processes.

Objective. The audit objective was to evaluate the effectiveness of the Y2K end-to-end tests planned for the logistics functional area. This report, the fifth in a series on logistics end-to-end testing, addresses the overall end-to-end test planning accomplished by the Navy.

Results. The Navy end-to-end test planning for core logistics processes generally met the requirements outlined in the DoD Management Plan and the Logistics Capstone Plan. In response to the practical limitations imposed by resource constraints and calendar time remaining, the core logistics processes and data flows were prioritized to determine which to include in testing. Five critical core logistics processes were identified for testing. The five core processes were requisition, shipment, receipt, inventory control, and asset status. The Navy tested three (requisition, receipt, and inventory control). The Navy included 8* of its 23 mission-critical systems listed in the DoD Y2K Reporting Database in functional area end-to-end testing. However, the Navy did not accurately track the test status of Navy mission-critical logistics systems and reconcile the systems with the DoD Y2K Reporting Database. For five systems, the Navy could not provide information on how or when the systems would be tested at a higher level. Further, the Navy did not provide the risk assessments prepared during the process of prioritizing logistics processes. As a result, there was no assurance that all mission-critical logistics systems will be tested as required. However, the Navy did plan to perform additional verification and validation of mission-critical code as funds are made available (finding A).

Adequate system contingency plans and operational contingency plans had not been written for all Navy mission-critical logistics systems, and 16 of the existing plans may not have been validated to verify that they are executable. As a result, the Navy Y2K Project Office was not effectively monitoring the completion and validation of both system contingency plans and operational contingency plans, and the capability of the Navy logistics community to respond effectively to unanticipated Y2K-related disruptions of logistics systems is at risk (finding B).

Summary of Recommendations. We recommend that the Chief Information Officer, Department of the Navy, determine the status of the five mission-critical logistics systems that were not recorded as having had higher level tests, test them as required, and update the DoD Y2K Reporting Database and the Naval Y2K Tracking System to reflect the status of testing of the system tested; complete risk management plans for all core logistics processes; and request additional funds for the second code scanning. We also recommend that the Chief Information Officer revise and publish the description, templates, and sample for system contingency plans in the Navy Year 2000 Contingency and Continuity of Operations Planning Guide; direct the Naval Sea Systems Command and the Naval Supply Systems Command to revise their contingency plans for mission-critical logistics systems; and revise the Navy Contingency Plan Status List.

Management Comments. The Chief Information Officer, Department of the Navy, did not comment on a draft of this report issued October 6, 1999. We request that the Chief Information Officer provide written comments on this final report by December 16, 1999.

---

* Seven systems were included in logistics Level II end-to-end testing and one was included in the procurement-financial end-to-end test.

Table of Contents

Executive Summary i

Introduction

Background 1
Objectives 2

Findings

A. Navy Planning for Logistics Functional End-to-End Testing 3
B. System Contingency Plans and Operational Contingency Plans 13

Appendixes

A. Audit Process
Scope and Methodology 23
B. Summary of Prior Coverage 25
C. Navy Mission-Critical Logistics Systems 26
D. Report Distribution 28

Background

Executive Order. Because of the potential failure of computers to function throughout the Government, the President issued Executive Order 13073, "Year 2000 Conversion," February 4, 1998, making it policy that Federal agencies ensure that no critical Federal program experiences disruption because of the year 2000 (Y2K) problem. The order requires that the head of each agency ensure that efforts to address the Y2K problem receive the highest priority attention in the agency.

Public Law. Public Law 105-261, "National Defense Authorization Act for Fiscal Year 1999," October 17, 1998, Section 334(b), directs that the Secretary of Defense ensure that "all mission critical systems that are expected to be used if the Armed Forces are involved in a conflict in a major theater of war are tested in at least two exercises." In addition, Section 334(d) states: "Alternative Testing Method. In the case of an information technology or national security system for which a simulated year 2000 test as part of a military exercise described in subsection (c) is not feasible or presents undue risk, the Secretary of Defense shall test the system using a functional end-to-end test or through a Defense Major Range and Test Facility Base."

DoD Y2K Management Strategy. In his role as the DoD Chief Information Officer, the Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), issued the "DoD Year 2000 Management Plan, Version 2.0" (DoD Management Plan) in December 1998. The DoD Management Plan required DoD Components to implement a five-phase (awareness, assessment, renovation, validation, and implementation) Y2K management process to be completed by December 31, 1998, for mission-critical systems.

The DoD Management Plan also provides guidance for implementing the Deputy Secretary of Defense memorandum, "Year 2000 (Y2K) Verification of National Security Capabilities," August 24, 1998, that requires that each Principal Staff Assistant (PSA) of the Office of the Secretary of Defense "verify that all functions under his or her purview will continue unaffected by Y2K issues." That verification was to be performed after completion of the five-phase management approach that culminated with completion of the implementation phase, December 31, 1998. That further testing, to be conducted during the first half of 1999, was planned and conducted from a mission perspective rather than a system perspective and would increase the confidence that any errors or omissions in system remediation would be found. The Deputy Under Secretary of Defense (Logistics) (DUSD[L]) acts on behalf of the Under Secretary of Defense for Acquisition, Technology, and Logistics, the PSA for logistics, in performing those functions for the logistics functional area.

DoD Logistics End-to-End Planning. The DUSD(L&MR) implemented and executed key components of the DoD Management Plan in his efforts to adequately plan for and manage logistics functional end-to-end testing. Test planning was accomplished through the "Logistics Capstone Operational

Assessment Plan for Year 2000" (Logistics Capstone Plan), dated October 30, 1998, and approved in November 1998. The Logistics Capstone Plan provided the overall strategy for conduct of the logistics end-to-end testing and was coordinated with the Services, the Defense Logistics Agency (DLA), the Joint Interoperability Test Command, and the Joint Staff. The October 1998 Logistics Capstone Plan was updated in February 1999 and again in May 1999 to reflect evolving schedules and processes. Its name was changed to "Logistics Capstone Plan for Year 2000 End-to-End Test" as part of the February update. In this report, unless otherwise noted, Logistics Capstone Plan refers to the May 20, 1999, version.

Objective

The audit objective was to evaluate the effectiveness of the Y2K end-to-end tests planned for the logistics functional area. This report, the fifth in a series on logistics end-to-end testing, addresses the overall end-to-end test planning accomplished by the Navy. See Appendix A for a discussion of the audit scope and methodology and Appendix B for a summary of prior coverage.

A. Navy Planning for Logistics Functional End-to-End Testing

The Navy end-to-end test planning for core logistics processes generally met the requirements outlined in the DoD Management Plan and the Logistics Capstone Plan. In response to the practical limitations imposed by resource constraints and calendar time remaining, the Navy and the other Services, in conjunction with the Logistics Y2K Interface Assessment Working Group,[1] the DUSD(L&MR), and DLA, prioritized the core logistics processes and data flows, based on criticality to the warfighter. They identified five critical core logistics processes for testing, and the Navy participated in three of the five processes. The Navy included 8[2] of its 23 mission-critical systems listed in the DoD Y2K Reporting Database in functional area end-to-end testing. However, the Navy did not accurately track the test status of Navy mission-critical logistics systems and reconcile the systems with the DoD Y2K Reporting Database. For five systems, Navy could not provide information on how or when the systems would be tested at a higher level. Further, the Navy did not provide the risk assessments prepared during the process of prioritizing logistics processes to the DUSD(L&MR) for inclusion in an overall risk management plan. As a result, there was no assurance that all mission-critical logistics systems will be tested as required. However, the Navy did plan to perform the verification and validation of mission-critical code as funds are made available.

DoD Guidance for End-to-End Testing

Test Plans. The Logistics Capstone Plan provided the overall strategy for conduct of the DoD logistics end-to-end testing. To ensure compliance with Logistics Capstone Plan requirements, the Navy published the "Year 2000 (Y2K) Capstone System Test Plan, Navy Software Test Plan (STP)," (the Navy Capstone Plan) April 17, 1999. The plan defines the Navy logistics systems to be tested, environment constraints, general test conditions, levels of testing, proposed test schedule, requirement traceablility, and test personnel. The purpose of the Navy Capstone Plan was to serve as a guide for testing of the Navy logistics systems within Navy and all interface testing required for Y2K certification. In July 1999, the Navy issued "Naval Year 2000 Master Test Plan," (Navy Test Plan) version 3.0, to synchronize all naval organizations

[1] The Logistics Y2K Interface Assessment Working Group membership was composed of DoD Component representatives and was chaired by the Director, Logistics Systems Modernization.

[2] Seven systems were included in logistics Level II end-to-end testing and one was included in the procurement-financial end-to-end test.

supporting the planning and execution of Y2K Integrated Testing and Fleet Validation to ensure a comprehensive, consistent, and efficient approach to Navy testing.

Navy Test Responsibilities. The Fleet Industrial Support Center, the Naval Inventory Control Point, Navy Central Design Activities at the Fleet Material Support Office, and the Space and Naval Warfare Systems Command (SPAWAR) were responsible for conducting qualification testing of the mission-critical thin lines.[3] Additionally, DLA and the other Services interfaced at various points along the mission-critical threads (a thread is a specified sequence of automated information systems required to accomplish a defined objective). Functional subject matter experts, computer programmers, and computer specialists from the responsible Navy organizations performed the Level II testing. The personnel had full knowledge of programs supporting the systems and associated applications and were capable of analyzing test input and output to ensure test objectives were achieved.

Navy Planning for End-to-End Testing

The Navy end-to-end test planning for critical core logistics processes generally met the requirements outlined in the DoD Management Plan and the Logistics Capstone Plan. The objective of Navy participation in the DoD logistics Level II end-to-end test effort was to determine whether Navy critical systems could interface correctly with other DoD systems in a Y2K environment. The specific objective was to verify information flows to and from each Service Component and DLA. As required by the Logistics Capstone Plan, the Navy Test Plan addressed areas such as end-to-end test strategy, critical core processes, mission-critical systems that support the core processes, and test limitations.

The Navy started end-to-end testing of its critical core processes and mission-critical systems on May 25, 1999, and completed the tests on July 14, 1999. The DoD Management Plan calls for final test reports to be completed within 30 days of completion of testing. The final report for Level II testing, "Logistics Year 2000 End-to-End Level II Exercise Evaluation Report," October 1999, by the independent evaluator, the Joint Interoperability Test Command, concluded that critical core processes will continue unaffected by Y2K issues. Anomalies were identified for one Navy mission-critical system, an end-of-decade anomaly for the Uniform Automated Data Processing System (UADPS), and for one non-mission-critical system, a Y2K anomaly for the Streamlined Automated Logistics Transmission System (SALTS). The operational impact of the UADPS non-Y2K-related anomaly was assessed as minimal and system representatives had a plan to revise the code and release a

[3] Thin lines refer to those automated systems that support the performance of the critical mission process.

production version by September 1999. The SALTS software was corrected and a patch for the system was developed and released to the field.

Testing Strategy. The Logistics Capstone Plan defines three levels of testing and delegates responsibility for each. The multilevel test approach consisted of intra-Component events (Level I), inter-Component events (Level II), and post-test activities that include retest (Level III). Level I tests were designed to ensure processes and systems within a Component's organizational boundaries are Y2K ready. Level II testing was to verify critical core processes and information flows that involved more than a single Component are Y2K ready. The execution and oversight of the Level I testing was completely delegated to the Components while DUSD(L&MR) focused on the Level II testing and post-test events, such as retest, during Level III. Independent validation and verification of Level II testing was achieved through the use of the Joint Interoperability Test Command for test planning, execution, and reporting. The Navy incorporated the guidelines from the Logistics Capstone Plan into the Navy Capstone Plan. The Navy further categorized the testing of its mission-critical systems, which support the warfighter, into three levels, each of which is composed of two phases.

- Level 1-Systems Certification. Phase 1 tests systems for Y2K compliance. Phase 2 includes laboratory testing to determine if the systems can interact with other systems within the organizational boundaries of commands or platforms while processing data correctly in a Y2K environment. Level 1 tests did not test operational readiness and were not equated to an operational or a functional end-to-end test.

- Level 2-Functional Testing. Phase 1 tests integrated functions within platforms in a laboratory environment. Phase 2 is composed of inter-platform tests aboard ships and at shore facilities in an operational environment.

- Level 3-Integration Validation. Phase 1 is made up of Battle Group Systems Integration Testing. Phase 2 is joint validation through end-to-end testing.

Core Processes. The Navy and the other Services, in conjunction with the Logistics Y2K Interface Assessment Working Group, the DUSD(L&MR), and DLA, agreed that all mission-critical systems and processes could not be assessed during the logistics functional Level II end-to-end testing because of time and resource constraints. They identified 8 out of 15 core supply and materiel management processes as mission-critical to the warfighter. The eight processes were further refined to reflect five processes to be included in the Level II end-to-end testing. The narrow focus for Level II logistics end-to-end testing was to assess core processes for functions that would impair a warfighting mission within hours or days of being needed and not available. The five core processes were requisition, shipment, receipt, inventory control, and asset status. The Navy participated in three of the five core processes tested during Level II end-to-end testing. The Navy did not participate in end-to-end

testing of the shipment process because the Navy portion of the shipment process is inherent in the requisition process. The Navy also did not participate in the asset status process because it was scheduled to be tested during other higher level tests. The general approach taken by the Navy, the other Services, and DLA was to identify critical functional processes and then the information systems that supported those processes. The Navy initially identified eight mission-critical systems for Level II testing that it used to support the three core logistics processes. Table 1 provides a list of those eight systems and shows their relationships to the processes that were included in Level II end-to-end testing. See Appendix C for a listing of the Navy mission-critical systems and the commands responsible for them.

Table 1. Navy Logistics Level II Testing

	Process		
System[1]	Requisition	Receipt	Inventory
NALCOMIS (OMA)[2]	X		
RAM[2]	X		
SNAP I (UNIX PORT)	X		
SNAP II (UNIX PORT)	X		
UADPS			
TANDEM			
(CPEN)[3]	X		
(DDA)[3]	X	X	X
UADPS(U2)	X	X	X
UICP-RESYS	X	X	X
UICP-TRANS	X	X	X

[1] These systems are defined in Appendix C.

[2] System was initially identified for testing, but was not tested. A different system was tested.

[3] CPEN and DDA are part of TANDEM and are counted as one system.

Test Limitations. Because all logistics processes and mission-critical system interfaces could not be tested within the time available, the Navy limited its testing in several areas, as described in the following paragraphs.

Test Environment. The Navy Level II end-to-end testing was performed to ensure interoperability in Y2K environments of mission-critical system interfaces. Testing included all files, interface control documents, and support utilities needed to validate the Logistics Capstone Plan. Level II end-to-end testing ensured that:

- all program support utilities functioned properly in the new Y2K environment,
- applications functioned and performed in the new Y2K environment using the dates identified for the intra-Navy and inter-Component tests,
- uploads and downloads of data functioned properly, and
- Y2K platforms met or exceeded the performance of the current operating environments without change to the system functionality.

The limitations in the Navy test environment are as follows.

- System testing will not validate the support utility programs.
- Tests will not be conducted in production environments[4] but will use representative test environments.
- The representative test environments have less memory capabilities than the production environments.
- Testing will not be an uninterrupted end-to-end test. Because the test environment could not be configured to simulate all systems at one time, the test will be configured to simulate each system sequentially.

Date Crossings. Date scenarios tested in Level II testing were fiscal year (September 30, 1999, to October 1, 1999), calendar year (December 31, 1999, to January 1, 2000), and leap day (February 28, 2000, to February 29, 2000, and February 29, 2000, to March 1, 2000). A baseline test was performed to compare current data with the test results.

Transactions. The Navy limited the number and type of transactions it tested in Level II end-to-end testing. The Navy selected supply transactions for nine equipment classes for end-to-end testing. The transactions included 82 Navy national stock numbers. Level II end-to-end testing confirmed accurate transmission of data from the Navy to the other Services and DLA. According

[4] Production environments are the environments in which software applications operate on a day-to-day basis.

to the October 1999 Joint Interoperability Test Command final report, all Navy transactions tested were fully successful.

Testing Status of Mission-Critical Systems

The Navy did not accurately track the test status of all Navy mission-critical logistics systems and reconcile the Naval Y2K Tracking System with the DoD Y2K Reporting Database. Also, for five of the systems shown in the Naval Y2K Tracking System as not having had higher level tests, naval personnel could not provide us information on how or when the systems would be tested. Further, the DoD Y2K Reporting Database and the Naval Y2K Tracking System were not updated for one logistics system that completed a non-logistics end-to-end test.

The DoD Management Plan requires DoD Components to gather and maintain a Y2K database. The DoD Y2K Reporting Database is the single official source to support senior DoD management and for reporting all mission-critical systems to the Office of Management and Budget. The DoD Y2K Reporting Database is used to identify mission-critical systems, their Y2K status, and which phase of the five-phase Y2K management process they are in.

Monitoring the Status of Mission-Critical Systems. The Naval Y2K Tracking System did not accurately reflect the test status of all Navy mission-critical logistics systems. The Naval Y2K Tracking System is used to report test status and progress of system validation. Every Navy system was to be included in the tracking system. As system hardware, software, and operating systems were made compliant, the tracking system was to be updated. The Naval Y2K Tracking System is one key tool of the Navy Y2K Project Office for ensuring that Navy tasks and systems are properly evaluated to ensure mission continuity and compliance with public law and the DoD Management Plan. The Naval Y2K Tracking System contains data on all Navy Y2K operational assessments, Y2K operational demonstrations, and functional end-to-end tests.

To determine whether testing had been conducted or planned for all mission-critical logistics systems, we reconciled the test status of mission-critical logistics systems contained in the DoD Y2K Reporting Database with the status listed in the Naval Y2K Tracking System and discussed the test status of the systems with DoD and Navy officials. As of July 29, 1999, the DoD Y2K Reporting Database contained 23 Navy mission-critical logistics systems. Table 2 shows the 23 systems' status by source of the information.

Table 2. Comparison of DoD Y2K Reporting Database, Naval Y2K Tracking System, and Audit Results

System Test Status	Mission-Critical Systems DoD	Mission-Critical Systems Navy	Audit Results
Level I testing only	0	2	2
Level II testing only	0	6	0
Level I and II testing	10	2	7
USTRANSCOM operational evaluation	2	1	1
Service-sponsored system integration test	0	3	3
Testing not required (retired and legacy systems)	4	4	4
No higher level testing	7	5	5
Non-logistics end-to-end test	0	0	1

As shown in Table 2, the Navy did not accurately track the test status of all Navy mission-critical logistics systems, and the information recorded in the DoD Y2K Reporting Database and the Naval Y2K Tracking System did not agree.

For five of the systems, shown in the Naval Y2K Tracking System as not having been tested at a higher level, naval personnel could not provide us information on how or when the systems would be tested. Those systems are described in the following paragraphs.

Commercial Asset Visibility. This system maintains visibility of assets while at commercial sites.

Micro Organizational Maintenance Management System. This system manages organization-level equipment configuration, equipment maintenance, and associated logistics support data. The information managed by the system enables overall visibility and evaluation of equipment availability, condition, maintainability, and reliability.

Navy Material Transportation Office Operations and Management Information System. This system provides a documentation link among the shipper, the trans-shipper, and the receiver.

Retail Ordnance Logistics Management System. This system combines the functionality of the standardized conventional ammunition automated inventory record, the fleet optical scanning ammunition marking system and the ordnance management systems.

Ship Configuration and Logistics Support/Configuration Data Manager's Database-Open Architecture and Revised Alternative Dataflow Communications. This system tracks the status and maintenance of naval equipment and related logistics items aboard ships and at naval organizations around the world.

The DoD Y2K Reporting Database and the Naval Y2K Tracking System were not updated for one logistics system that completed a non-logistics end-to-end test: the Advanced Traceability and Control-Navy system. That system maintains visibility and control of depot-level repairable items of supply until a decision is made to ship them to a depot for repair. The system was listed as a mission-critical logistics system on both the DoD Y2K Reporting Database and the Naval Y2K Tracking System, but there was no indication that the system had been tested in end-to-end testing. On August 8, 1999, the Functional Integration Office, Naval Supply Systems Command (NAVSUP), stated that the system was a logistics system but that its critical interfaces were to Navy procurement and financial systems and not to other logistics systems. The Navy had tested the system as part of the procurement-financial end-to-end test.

Measures to Minimize Risk of Y2K-Related System Failures

Risk Assessments. The Navy did not provide the risk assessments performed during the process of prioritizing logistics processes for inclusion in end-to-end testing as required by the DoD Management Plan. The DoD Management Plan states that the Y2K event master planning sessions were to identify and prioritize core processes and perform risk assessments. The Logistics Capstone Plan identified four general categories of corporate-level risk: scope of testing; test environment; scheduling; and funding. It also assigned each category a risk rating of high, medium, or low, based on probability of occurrence and consequences of occurrence, and listed the mitigation for a particular risk. The Logistics Capstone Plan stated that the discussion of corporate-level risks was an initial risk assessment. In addition, the Logistics Capstone Plan stated that a complete risk mitigation plan will be incorporated in an overall risk management plan. The DUSD(L&MR) had planned to complete an overall risk management plan in September 1999. The Navy Test Plan included guidance on preparing and submitting a risk management plan to the DUSD(L&MR) for the Navy mission-critical processes and systems. The Navy Y2K Project Office stated that the system risk assessments were prepared in conjunction with the

contingency plans and the continuity of operations plans. As of September 30, 1999, however, the Navy had not forwarded a completed risk management plan for review and inclusion in the overall DUSD(L&MR) risk management plan.

Additional Navy Measures to Mitigate Risk. In addition to participating in end-to-end testing of the identified critical core logistics processes, the Navy Chief Information Officer took steps to minimize risk of critical logistics processes not functioning in the year 2000 by issuing policy guidance on Y2K independent validation and verification of automated information systems.

The Navy was providing code scanning capability for mission-critical systems. Although NAVSUP code had already undergone code scanning using IMPACT 2000, NAVSUP requested that mission-critical systems also be scanned using Crystal Systems Solutions' CodeMill because it is a later generation and, therefore, has more capability than IMPACT 2000. The second code scanning was underway; a portion of the code had been scanned a second time. As of September 9, 1999, the Functional Integration Office, NAVSUP, stated that an additional 9 million lines of code had been forwarded to the Navy Y2K Project Office and would be scanned as funds were available.

The code scanning effort initiated by the Navy should assist in uncovering remaining Y2K errors and provide system managers the opportunity to validate and fix those errors, as well as retest systems as needed.

Conclusion

The Navy generally complied with the DoD Management Plan and the Logistics Capstone Plan to plan and manage its portion of the logistics Level II end-to-end testing. Although 15 core logistics processes were identified during the DoD planning process, the Navy only participated in 3 of the 5 core processes that were included in Level II end-to-end testing. Planning officials acknowledged that time and resource constraints played a role in limiting the number of processes to be tested; however, limiting Level II testing to three core processes presents some risk that other processes will not be adequately tested. Because the Navy had not forwarded a completed risk management plan for review and inclusion in the overall DUSD(L&MR) risk management plan, the DUSD(L&MR) did not have sufficient information to complete a risk management plan for all core logistics processes by September 1999 and may not be able to meet the revised goal of November 1999.

Recommendations

A. We recommend that the Chief Information Officer, Department of the Navy:

1. Determine the status of the five mission-critical logistics systems that were not recorded as having had higher level tests and test them as required.

2. Update the DoD Year 2000 Reporting Database and the Naval Year 2000 Tracking System to reflect the status of testing of the system tested as part of the procurement-financial end-to-end test.

3. Complete and forward risk management plans for all core logistics processes to the Deputy Under Secretary of Defense (Logistics).

4. Request that the Secretary of the Navy provide funds for the second code scanning.

Management Comments Required

The Navy did not comment on a draft of this report. We request that the Chief Information Officer, Department of the Navy, provide comments on the final report.

B. System Contingency Plans and Operational Contingency Plans

Adequate system contingency plans and operational contingency plans had not been written for all Navy mission-critical logistics systems, and 16 of the existing plans may not have been validated to verify that they are executable. Adequate plans had not been written or validated because the Logistics Capstone Plan and Navy guidance on contingency plans were inconsistent with the requirements of the DoD Management Plan. Additionally, the Navy Contingency Plan Status List did not differentiate between system contingency plans and operational contingency plans, did not indicate whether the plans had been reviewed for adequacy, and did not indicate whether the plans had been validated in accordance with the requirements of the DoD Management Plan. As a result, the Navy Y2K Project Office was not effectively monitoring the completion and validation of both system contingency plans and operational contingency plans, and the capability of the Navy logistics community to respond effectively to unanticipated Y2K-related disruptions of logistics systems is at risk.

DoD Management Plan

The DoD Management Plan describes the difference between system contingency plans and operational contingency plans, which are also called continuity of operations plans. System contingency plans address processes and procedures for restoring functionality to a disrupted system. System contingency plans address activities to be performed by the system administrator or local area network manager to preserve and protect the system and its data. Operational contingency plans identify alternative systems or procedures (workarounds) for operational commanders and staff to use, when performing a mission or function, if a primary system is disrupted.

The DoD Management Plan also states that contingency plans must be validated to ensure that alternatives are realistic and executable. The plans for mission-critical systems are to be tested during Y2K operational or end-to-end exercises. The target date for exercising both mission-critical system contingency plans and operational contingency plans was June 30, 1999. The DoD Management Plan also states that when contingency plans are not tested during operational or end-to-end exercises, a subjective validation is to be conducted to:

- verify contingency procedures are correct,
- verify contingency actions are executable,
- verify that all personnel understand their roles and can execute their responsibilities,

- verify information in the plan is current and accurate,
- verify that personnel involved in execution and recovery have training available, and
- identify deficiencies in the plan.

The results of contingency plan tests or validations should be documented in exercise evaluation reports, according to the DoD Management Plan.

Mission-Critical System and Operational Contingency Plans

Adequate system contingency plans and operational contingency plans had not been written as of August 12, 1999, for all Navy mission-critical logistics systems, and 16 of the existing plans may not have been validated to verify that they are executable.

Contingency Plan Content. Navy commands did not clearly differentiate between plans, and it was difficult to determine whether the plans were system contingency plans, operational contingency plans, or a combination of both. The plans for all 19 Navy mission-critical logistics systems[5] were identified as system contingency plans in the Navy Contingency Plan Status List maintained by the Navy Y2K Project Office. However, only the Naval Sea Systems Command (NAVSEA) plan for the Ship Configuration and Logistics Support/Configuration Data Manager's Database-Open Architecture and Revised Alternative Dataflow Communications system specifically stated that it was a system contingency plan and that local site or agency operational contingency plans were needed.

All of the plans for the 19 mission-critical logistics systems were forwarded by us to the Director, Contingency Planning, in the Year 2000 office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (Y2K Office) for review and comment. The Director's staff determined that not all of the plans contained the minimum elements of a system contingency plan, as described in the DoD Management Plan. The Director's staff determined that the plans applicable to seven SPAWAR systems listed as system contingency plans contained at least some descriptions of what a system administrator must do to restore system functionality, as required by the DoD Management Plan. Most of the 19 plans also contained at least some references to workaround procedures for operational commanders to use if a primary system is disrupted, as required by the DoD Management Plan for operational contingency plans. The Director's staff stated that the seven SPAWAR plans

[5] Although the DoD Y2K Reporting Database listed 23 mission-critical logistics systems, 2 systems did not require testing because they were legacy systems and were to be replaced and another 2 systems did not require testing because they were to be retired and would not be replaced.

were good examples of combined system and operational contingency plans. The seven plans provided the most useful information to restore system hardware, software, and operational workarounds to perform mission requirements until the system could be restored to functionality.

However, the Director's staff stated that the plans for the 12 NAVSEA and NAVSUP systems needed to be revised in order to adequately reflect the requirements of the DoD Management Plan. For example, the NAVSEA contingency plan for the Conventional Ammunition Integrated Management System (CAIMS) was identified as an operational contingency plan on the title page, but contained a statement, normally applicable to a system contingency plan, that the plan addressed actions to be taken by the CAIMS Project Office to minimize system downtime in the event of a system failure. However, the plan contained no specifics as to what the CAIMS Project Office system administrator must do to restore the CAIMS system to functionality.

Table 3 shows whether the Director's staff considered contingency plans for Navy mission-critical logistics systems to be adequate.

Table 3. Navy Logistics Contingency Plans by Command

Command	System*	Adequate Contingency Plan	Inadequate Contingency Plan
NAVSEA	CAIMS		X
	DTTS		X
	ROLMS		X
	SCLSIS/CDMD-OA/RADCOM		X
NAVSUP	ATAC-NVY		X
	CAV		X
	NAOMIS		X
	RAM		X
	UADPS TANDEM		X
	UADPS(U2)		X
	UICP-RESYS		X
	UICP-TRANS		X
SPAWAR	AV3M	X	
	MOMMS	X	
	NALCOMIS IMA	X	
	NALCOMIS OMA	X	
	NTCSS-DANA	X	
	SNAP I (UNIX PORT)	X	
	SNAP II (UNIX PORT)	X	

*These systems are defined in Appendix C.

The plans applicable to the eight NAVSUP systems listed in Table 3 contained very limited descriptions of operational workaround procedures and no specifics as to what a system administrator must do to restore the system to functionality. For example, the plans instruct users to "invoke established local operating procedures and/or local continuity of operations plans while the system is offline. Local operating procedures should include manual submission and processing of requisitions via bearer walk through, telephone, fax or internet." An untitled continuity of operations plan is also referenced in each plan.

Validation and Testing. NAVSEA provided documentation that some type of contingency plan validation had been conducted for three of the four plans listed in Table 3. One system contingency plan, for the Retail Ordnance Logistics Management System, was included in a shipboard exercise. However, the Navy message from that ship did not describe how the plan was exercised or the organizations that were involved. The documentation concerning the Ship

Configuration and Logistics Support/Configuration Data Manager's Database-Open Architecture and Revised Alternative Dataflow Communications system did not indicate that the system had been validated by any of the methods described in the DoD Management Plan. The NAVSUP contingency plans did not contain a requirement for validating or testing, and command officials did not provide documentation of any testing. None of the NAVSUP plans contained a requirement to document or report the results of plan testing, as required by the DoD Management Plan. All of the latest versions of system contingency plans for SPAWAR logistics systems stated that testing was to be accomplished during shipboard fast cruise and end-to-end exercises. However, SPAWAR officials did not provide documentation of any plans tested during shipboard fast cruise exercises. Navy contingency plans were not tested during the intra-Navy end-to-end exercise conducted from April 12, 1999, through May 14, 1999, or during the DoD Y2K logistics end-to-end exercise conducted from May 25, 1999, through July 14, 1999.

Comparison of Guidance

Adequate plans had not been written or validated because the Logistics Capstone Plan and Navy guidance on contingency plans were inconsistent with the requirements of the DoD Management Plan.

Logistics Capstone Plan. The Logistics Capstone Plan did not address the difference between system contingency plans and operational contingency plans. The Logistics Capstone Plan requires only that, at a minimum, all thin lines supporting mission-critical logistics processes have an effective contingency plan.

Navy Test Plan. The guidance on contingency plans in the Navy Test Plan was inconsistent with the requirements of the DoD Management Plan. The guidance in the Navy Test Plan states that system contingency plans and operational contingency plans are to be tested when technical solutions are uncertain or not feasible. Testing of contingency plans during Battle Group Systems Integration Testing would be limited to systems that fail or show an abnormality, according to the Navy Test Plan. The Navy Test Plan requires documentation "of all facets of the test process." However, the Navy Test Plan is not clear whether results of contingency plan tests or validation are included in the documentation requirement. Also, the Navy Test Plan does not specify a completion date for the testing, and does not address how other mission-critical systems will be tested. Additionally, the Navy Test Plan guidance on system contingency plan testing incorrectly states that contingency plans need to be tested to inform system users of possible workarounds. That is the primary purpose of operational contingency plans, not system contingency plans.

Navy Contingency Planning Guide. The guidance on system contingency plans in the "Navy Year 2000 Contingency and Continuity of Operations Planning Guide," (Navy Contingency Planning Guide) November 1, 1998, is

inconsistent with the requirements of the DoD Management Plan. The Navy Contingency Planning Guide states that a contingency plan may cover a number of systems, grouped into a family of related systems that support a functional area. The Navy Contingency Planning Guide includes separate appendixes describing the required elements of system contingency plans versus operational contingency plans and includes templates and sample system contingency plans and operational contingency plans. However, the appendixes, templates, and sample for a system contingency plan focus on alternatives for users to follow if a system fails and do not address what a system administrator must do to restore system functionality, as required by the DoD Management Plan. For example, the CAIMS plan closely followed the sample system contingency plan in the Navy Contingency Planning Guide. The CAIMS plan contains a reprint of instructions for developing alternative strategies from the Navy Contingency Planning Guide, which includes the following strategies for a partial or total system failure.

- Establish help desk.
- Use established emergency correction procedures.
- Identify workarounds.
- Operate manually until workarounds are implemented.
- Perform daily database backups.

The Navy guidance on contingency plan testing (validation) is also inconsistent with the requirements of the DoD Management Plan. For example, the Navy Contingency Planning Guide, Appendix A, "Contingency Plans for Mission Critical Systems," states that "[t]o the extent practical, contingency plans should be tested and rehearsed regularly." The only reference to a specific time period for completing system contingency plan tests is in the sample system contingency plan. The sample states that if no system failure occurs during shipboard Y2K testing, the procedures in the contingency plan are to be tested at one shore facility and one ship in June 1999.

The Navy Contingency Planning Guide was forwarded along with copies of the contingency plans to the Director, Contingency Planning, Y2K Office, for review and comment. The Director's staff stated that the appendixes, templates, and sample for system contingency plans in the Navy Contingency Planning Guide needed to be revised to conform to the requirements of the DoD Management Plan. The Director's staff also recommended that system contingency plans contain references to the system maintenance and technical manuals.

The Navy Contingency Planning Guide information on the testing of operational contingency plans was much more specific and comprehensive. For example, Appendix B, "Continuity of Operations Plans (Afloat)" states:

> Operational contingency plans must be tested/exercised to the maximum extent possible during fast cruise, inport training events, underway operations, fleet/joint exercises and Battle Group Systems Integration Testing (BGSIT). It is mandatory for all operational contingency plans to be tested/exercised during the Y2K phase of [the] Final Integration Testing portion of the BGSIT. It is recommended that lessons learned during BGSIT be extensively used to update/refine operational contingency plans.

Navy Contingency Plan Status List

The Navy Contingency Plan Status List did not differentiate between system contingency plans and operational contingency plans, did not indicate whether the plans had been reviewed for adequacy, and did not indicate whether the plans had been validated in accordance with the requirements of the DoD Management Plan. Navy Y2K Project Office officials stated that the purpose of the list, which as of August 8, 1999, had been last updated in February 1999, was to indicate whether a contingency plan had been prepared for each mission-critical system and whether the plan had been received by the Navy Y2K Project Office. The list indicated that contingency plans for all of the 19 mission-critical logistics systems had been received by the Navy Y2K Project Office. However, Navy Y2K Project Office officials were unable to confirm whether the plans received had been reviewed for adequacy, as required by the DoD Management Plan.

Additionally, the Navy Contingency Plan Status List did not indicate whether the plans had been validated in accordance with the DoD Management Plan. For example, a CAIMS contingency plan validation exercise was conducted on June 8 and June 9, 1999, in Mechanicsburg, Pennsylvania, but as of August 8, 1999, there was no data field on the Navy Contingency Plan Status List to record that validation.

Monitoring Plans and Capability to Respond

The Navy Y2K Project Office was not effectively monitoring the completion, adequacy, and validation of both system contingency plans and operational contingency plans, and the capability of the Navy logistics community to respond effectively to unanticipated Y2K-related disruptions of logistics systems is at risk. A Navy Contingency Plan Status List had been created as a management tool. However, as of August 8, 1999, the list did not provide Navy Y2K Project Office managers with sufficient information to determine that adequate system and operational contingency plans were available so that administrators and users of NAVSEA and NAVSUP mission-critical logistics systems could respond effectively to unanticipated Y2K-related disruptions. The list also did not provide Navy Y2K Project Office managers with sufficient

information to determine whether contingency plans had been reviewed for adequacy and validated to verify that they are executable, in accordance with the requirements of the DoD Management Plan.

Management Actions

Management emphasis is now focused on operational contingency plans. The Y2K Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) developed and issued an Operational Contingency Plan Review Worksheet on August 4, 1999. The worksheet requires that reviewers determine whether each plan exceeds or meets minimum criteria and whether improvements are recommended. The following criteria categories are to be reviewed.

- Statement of Purpose and Scope of Plan
- Description of Systems Supporting a Plan
- Roles and Responsibilities Under This Plan
- Vulnerabilities and Risk Analysis
- Descriptions of Contingency Actions
- Contingency Action Implementation and Coordination
- Plan Validation and Maintenance
- Documentation and Reporting Requirements

The Navy Y2K Project Office published a draft Contingency Planning/ Consequence Management Plan, July 27, 1999, that reiterates the Navy Contingency Planning Guide validation requirements for operational contingency plans and states that all operational contingency plan validations are to be completed by September 30, 1999. The draft plan also states that the method used to validate an operational contingency plan and a summary of the validation, including any plan modification recommendations, are to be reported.

The Navy Y2K Project Office also issued guidance to clarify the DoD Management Plan and Navy requirements for both system contingency plans and operational contingency plans. The Navy Y2K Project Office also requested the following information for all Navy system contingency plans and operational contingency plans by August 6, 1999:

- a listing of existing Y2K system and operational contingency plans,

- dates that system and operational contingency plans were validated, and
- whether DoD Management Plan validation requirements were used.

Recommendations

B. We recommend that the Chief Information Officer, Department of the Navy:

1. Revise the appendixes, templates, and sample for system contingency plans in the Navy Year 2000 Contingency and Continuity of Operations Planning Guide to conform to the requirements of the DoD Year 2000 Management Plan, and publish the revised guide as soon as possible.

2. Direct the Naval Sea Systems Command and the Naval Supply Systems Command year 2000 officials to revise and validate their contingency plans for mission-critical logistics systems to conform to the requirements of the DoD Year 2000 Management Plan and provide copies of the revised plans to the Navy Year 2000 Project Office.

3. Revise the Navy Contingency Plan Status List to document:

a. Whether both a system contingency plan and an operational contingency plan exist for each mission-critical logistics system or family of systems.

b. Whether the mission-critical logistics system contingency plans and operational contingency plans have been reviewed for adequacy in accordance with the requirements of the DoD Year 2000 Management Plan.

c. Whether the mission-critical logistics system contingency plans and operational contingency plans have been validated in accordance with the requirements of the DoD Year 2000 Management Plan.

4. Require all fleet and system command year 2000 officials to use the Operational Contingency Plan Review Worksheet developed by the Year 2000 office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to document the adequacy of operational contingency plans for each mission-critical logistics system or family of systems.

Management Comments Required

The Navy did not comment on a draft of this report. We request that the Chief Information Officer, Department of the Navy, provide comments on the final report.

Appendix A. Audit Process

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

Scope and Methodology

Work Performed. We reviewed the Y2K test planning efforts of the Navy for the logistics functional end-to-end testing. We evaluated the Y2K planning efforts of the Navy and compared those efforts with the criteria contained in the DoD Management Plan. We reviewed Public Law 105-261, Section 334; the Deputy Secretary of Defense memorandum of August 24, 1998; the DoD Management Plan; the Logistics Capstone Plan; the Navy Test Plan; the Navy Capstone Plan; and other guidance regarding the testing of mission-critical logistics systems. Documents reviewed were dated from November 1998 through September 1999. We interviewed personnel within the Office of the DUSD(L&MR), the Department of Navy, and the Office of the Chief Information Officer. We also interviewed the contractor representative involved with logistics end-to-end testing.

DoD-Wide Corporate-Level Goals. In response to the Government Performance and Results Act, DoD established 2 DoD-wide corporate-level performance objectives and 7 subordinate performance goals. This report pertains to achievement of the following goal and subordinate performance goal.

> **Goal 2:** Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs and reengineering the Department to achieve a 21st century infrastructure. **Performance Goal 2.2:** Transform U.S. military forces for the future. **(00-DoD-2.2)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following objectives and goals in the Information Technology Management Functional Area.

- **Objective:** Become a mission partner.
  Goal: Serve mission information users as customers. **(ITM-1.2)**

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

- **Objective:** Provide services that satisfy customer information needs. **Goal:** Upgrade technology base. **(ITM-2.3)**

High-Risk Area. In its identification of risk areas, the General Accounting Office has specifically designated risk in resolution of the Y2K problem as high. This report provides coverage of that problem and of the overall Information Management and Technology high-risk area.

Audit Type, Dates, and Standards. We performed this program audit from June through August 1999 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did not use computer-processed data for this audit.

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

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness area in the FY 1998 Annual Statement of Assurance.

Appendix B. Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Inspector General, DoD, reports can be accessed over the Internet at http://www.dodig.osd.mil. The reports most relevant to the subject matter of this report are listed below.

General Accounting Office

General Accounting Office Report No. GAO/AIMD-99-172 (OSD Case No. 1823), "Defense Computers: Management Controls Are Critical to Effective Year 2000 Testing," June 30, 1999.

Inspector General, DoD

Inspector General, DoD, Report No. D-2000-036, "Defense Logistics Agency Logistics Year 2000 End-to-End Test Planning," November 12, 1999.

Inspector General, DoD, Report No. D-2000- , "Army Logistics Year 2000 End-to-End Test Planning," November 5, 1999.

Inspector General, DoD, Report No. 00-021, "Air Force Logistics Year 2000 End-to-End Test Planning," October 26, 1999.

Inspector General, DoD, Report No. 00-002, "Year 2000 End-to-End Testing: Logistics Capstone Plan," October 1, 1999.

Appendix C. Navy Mission-Critical Logistics Systems

Acronym	System Nomenclature	Command
ATAC-NVY	Advanced Traceability and Control-Navy	NAVSUP
AV3M	Aviation Maintenance Material Management	SPAWAR
CAIMS	Conventional Ammunition Integrated Management System	NAVSEA
CAV	Commercial Asset Visibility	NAVSUP
DTTS	Defense Transportation Tracking System	NAVSEA
LVLII[1]	Level II Uniform Automated Data Processing System	Not applicable
MOMMS	Micro Organizational Maintenance Management System	SPAWAR
NALCOMIS IMA	Naval Aviation Logistics Command/ Management Information System Intermediate Maintenance Activity	SPAWAR
NALCOMIS OMA	Naval Aviation Logistics Command/ Management Information System Organizational Maintenance Activity	SPAWAR
NAOMIS	Navy Material Transportation Office Operations and Management Information System	NAVSUP
NTCSS-DANA	Navy Tactical Command Support System-DANA Desktop Environment	SPAWAR
RAM	Residual Asset Management	NAVSUP
ROLMS	Retail Ordnance Logistics Management System	NAVSEA

[1] This system is being retired and will not be replaced.

Acronym	System Nomenclature	Command
SCLSIS/CDMD-OA/RADCOM	Ship Configuration and Logistics Support/ Configuration Data Manager's Database-Open Architecture and Revised Alternative Dataflow Communications	NAVSEA
SNAP I[2]	Shipboard Non-Tactical Automated Data Processing System I	SPAWAR
SNAP I (UNIX PORT)	Shipboard Non-Tactical Automated Data Processing System I (UNIX Port)	SPAWAR
SNAP II[2]	Shipboard Non-Tactical Automated Data Processing System II	SPAWAR
SNAP II (UNIX PORT)	Shipboard Non-Tactical Automated Data Processing System II (UNIX Port)	SPAWAR
TVIS[1]	Transportation Visibility Information System	Not applicable
UADPS TANDEM	Uniform Automated Data Processing System Tandem Platform	NAVSUP
UADPS(U2)	Uniform Automated Data Processing System IBM Platform	NAVSUP
UICP-RESYS	Uniform Automated Data Processing System for Inventory Control Point Resystemization	NAVSUP
UICP-TRANS	Uniform Automated Data Processing System for Inventory Control Point Transition	NAVSUP

[1] This system is being retired and will not be replaced.

[2] This system is a legacy system that will be replaced before January 1, 2000.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
  Deputy Under Secretary of Defense (Logistics and Materiel Readiness)
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
    Principal Director for Year 2000

Joint Staff

Director, Joint Staff

Department of the Army

Chief Information Officer, Army
Auditor General, Department of the Army
Inspector General, Department of the Army

Department of the Navy

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

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer, Air Force
Auditor General, Department of the Air Force
Inspector 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. Central Command
Commander in Chief, U.S. Transportation Command
  Commander, Military Traffic Management Command

Other Defense Organizations

Director, Defense Contract Audit Agency
  Chief Information Officer, Defense Contract Audit Agency
Director, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
  Chief Information Officer, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
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
  National Security Division Special Projects Branch
Federal Chief Information Officers Council
General Accounting Office
  National Security and International Affairs Division
    Technical Information Center
  Accounting and Information Management Division
    Director, Defense Information and Financial Management Systems

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Technology Problem
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd)

House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Committee on Science

Audit Team Members

The Readiness and Logistics Support Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

Shelton R. Young
Tilghman A. Schraden
Mary E. Geiger
David L. Leising
Woodrow W. Mack