

Audit



Report

SPACE AND NAVAL WARFARE SYSTEMS COMMAND
PREPARATIONS FOR YEAR 2000 BATTLE GROUP SYSTEMS
INTEGRATION TESTING

Report No. 99-171

May 26, 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

BGSIT	Battle Group Systems Integration Testing
BG	Battle Group
COOP	Continuity-of-Operations Plan
SPAWAR	Space and Naval Warfare Systems Command
SYSCOM	Systems Command
Y2K	Year 2000



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



May 26, 1999

MEMORANDUM FOR ASSISTANT SECRETARY OF THE NAVY (FINANCIAL
MANAGEMENT AND COMPTROLLER)

SUBJECT: Audit Report on Space and Naval Warfare Systems Command Preparations
for Battle Group Systems Integration Testing (Report No. 99-171)

We are providing this report for information and use. We considered management comments on a draft of this report in preparing the final report. Management comments conformed to DoD Directive 7650.3; therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Robert K. West at (703) 604-8983 (DSN 664-8983) (rwest@dodig.osd.mil) or Mr. Robert W. Otten at (703) 604-8997 (DSN 664-8997) (rotten@dodig.osd.mil). See Appendix C for the report distribution. The audit team members are listed inside the back cover.

A handwritten signature in black ink that reads "David K. Steensma".

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-171
(Project No. 9AD-0078)

May 26, 1999

Space and Naval Warfare Systems Command Preparations for Year 2000 Battle Group Systems Integration Testing

Executive Summary

Introduction. This report is one in a series of reports that the Inspector General, DoD, is issuing in accordance with an informal partnership with the DoD Chief Information Officer to monitor DoD efforts to address the year 2000 computing challenge.

The Battle Group Systems Integration Testing is an existing Navy process and was expanded in scope to address year 2000 concerns. The Battle Group Year 2000 Systems Integration Testing is designed to validate the Battle Group year 2000 readiness in an operational environment and to identify year 2000 interoperability issues. The Navy conducted the first Battle Group Year 2000 System Integration Testing on the U.S.S. *Constellation* Battle Group from February 28, 1999, through March 4, 1999. The Navy plans to conduct four additional Battle Group Year 2000 Systems Integration Tests before the year 2000.

Objectives. The overall audit objective was to evaluate whether the Space and Naval Warfare Systems Command effectively prepared for the U.S.S. *Constellation* Battle Group Systems Integration Testing for the year 2000 impact and to make recommendations for improving future Battle Group Year 2000 Systems Integration Testing. The audit focused on mission-critical systems that required a year 2000 renovation to be installed on ships in the U.S.S. *Constellation* Battle Group. Specifically, we reviewed the planning and installing of year 2000 renovations, initialization procedures, and contingency plans.

Results. The Space and Naval Warfare Systems Command processes for preparing for the U.S.S. *Constellation* Battle Group Systems Integration Testing for the year 2000 needed improvement. The Space and Naval Warfare Systems Command established the Year 2000 War Room to coordinate year 2000 management activities and developed a comprehensive timeline summary to monitor and track the installation of year 2000 renovations. Although the Space and Naval Warfare Systems Command identified systems that were not renovated and installed in time for the U.S.S. *Constellation* Battle Group Systems Integration Testing, it must make every effort to install and test those systems in future Battle Groups. See Appendix B for Other Matters of Interest.

The Space and Naval Warfare Systems Command initialization procedures did not address all required elements. As a result, future battle group systems integration testing managers may not have sufficient steps to validate systems in a year 2000 environment (Finding A).

Contingency plans did not provide specific procedures, and a contingency plan had not been prepared for the Contingency Theater Automated Planning System. Properly prepared contingency plans are essential to maintain mission capability, to restore systems to full operational capability efficiently and effectively, and to provide the ship force with contingency actions that are well defined, documented, tested, and feasible (Finding B).

Summary of Recommendations. We recommend a more effective quality assurance process to review initialization procedures and contingency plans and preparation of a contingency plan for the Contingency Theater Automated Planning System.

Management Comments. The Navy concurred with all recommendations and initiated a quality assurance process for initialization procedures and contingency plans. In June 1999, the Navy plans to replace the Contingency Theater Automated Planning System with a system that is year 2000 compliant. See the Findings section for a discussion of the management comments and the Management Comments section for the complete text of the comments.

Table of Contents

Executive Summary	i
Introduction	
Background	1
Objectives	3
Findings	
A. Year 2000 Initialization Procedures for Vulnerable Systems	4
B. Contingency Planning	7
Appendixes	
A. Audit Process	
Scope	16
Methodology	17
Summary of Prior Coverage	17
B. Other Matters of Interest	18
C. Report Distribution	20
Management Comments	
Department of the Navy Comments	23

Background

Year 2000 Battle Group Systems Integration Testing. The Battle Group (BG) Systems Integration Testing is an existing Navy process and was expanded in scope to address year 2000 (Y2K) concerns. The BG Y2K Systems Integration Testing (BGSIT) is designed to validate the BG Y2K readiness in an operational environment and to identify Y2K interoperability issues. The Navy conducted the first Y2K BGSIT on the U.S.S. *Constellation* Battle Group from February 28, 1999, through March 4, 1999. The Navy plans on conducting four additional Y2K BGSITs on four other BGs before the year 2000.

Space and Naval Warfare Systems Command Mission. The Space and Naval Warfare Systems Command (SPAWAR) designs, acquires, and supports systems that collect, coordinate, process, analyze, and present complex information to the warfighter. SPAWAR provides management information systems and communications applications for force-wide combat support systems. The systems allow commanders to integrate tactical information with key combat support logistics data in both joint and coalition warfare environments. SPAWAR also develops and acquires undersea surveillance systems, global weather and oceanographic forecasting systems, and navigational systems.

The Y2K Problem. The Y2K problem is the term most often used to describe the potential failure of information technology systems to process or perform date-related functions before, on, or after the turn of the century. Because of the potential failure of computers to run or function throughout the Government, the President issued an Executive Order, "Year 2000 Conversion," February 4, 1998. The executive order makes it policy that Federal agencies ensure that no critical Federal program experiences disruption because of the Y2K problem and that the head of each agency ensure that efforts to address the Y2K problem receive the highest priority attention in the agency.

DoD Y2K Management Plan. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), in his role as the DoD Chief Information Officer, initially issued the "DoD Year 2000 Management Plan" (DoD Management Plan) in April 1997. The latest version was signed on December 31, 1998. The DoD Management Plan provides the overall DoD strategy and guidance for inventorying, prioritizing, repairing, or retiring systems, and monitoring Y2K progress. The DoD Management Plan states that the DoD Chief Information Officer has overall responsibility for overseeing the DoD solution to the Y2K problem.

Navy Strategy. The Navy prepared and issued a Year 2000 Action Plan, a Y2K Contingency and Continuity-of-Operations Planning Guide, and a Naval Y2K Master Test Plan to outline the Navy Y2K management effort and strategy and to define Y2K roles, responsibilities, and reporting requirements. Although the Navy placed strong emphasis on mission-critical systems, its goal is to evaluate all Y2K vulnerable systems and equipment and to renovate those systems and equipment that have a Y2K concern.

Department of the Navy Year 2000 Action Plan. The Navy Y2K Action Plan, published in September 1998, provides the Navy strategy and management approach to addressing the Y2K date processing problem in the Navy. Specifically, it provides guidance for inventorying systems, prioritizing systems, retiring systems, and monitoring Y2K progress.

Navy Y2K Contingency and Continuity-of-Operations Planning Guide. The Navy Y2K Project Office published the Navy Y2K Contingency and Continuity-of-Operations Planning Guide on November 1, 1998, to help ensure that no loss of mission capability would result from a Y2K problem. The planning guide assists afloat and ashore Navy organizations and units in the identification and revision of existing contingency planning and continuity-of-operations efforts. The planning guide addresses the key elements of the Navy Y2K strategy to contingency planning and continuity of operations, and the roles and responsibilities of the Navy Commands. It is the responsibility of the system owners to prepare accurate and functional contingency plans and the responsibility of Navy managers and users to prepare, distribute, and test continuity-of-operations plans.

Naval Y2K Master Test Plan. The Navy Y2K Project Office published the Naval Y2K Master Test Plan on August 20, 1998. The Navy developed a multitiered, three-level test strategy to ensure the operational readiness of its critical functions and mission capabilities before, on, and after the year 2000. The three test levels are systems certification, functional testing, and integration validation. At level I (system certification), all systems are evaluated for possible Y2K problems at the intra-ship level. At level II, functional testing is planned to ensure that needed operational capabilities to support warfighter missions are maintained throughout the Fleet at the inter-ship level. Level II emphasizes the end-to-end testing of high technical risk Y2K renovations and testing of systems that provide the basic operational functionalities. Level III is a validation of the final system integration on a task-force level, including Battle Groups, Expeditionary Warfare Groups/Amphibious Ready Groups, Middle Eastern forces, and other deployers. Level III testing is done in concert with BGSIT and Final Integration Testing.

Y2K BGSIT Limitations. The U.S.S. *Constellation* BGSIT conducted only a Y2K rollover test, in which it would roll over the clock from December 31, 1999, to January 1, 2000, and did not conduct any other critical Y2K date tests. Commander-in-Chief, U.S. Pacific Fleet, Y2K officials stated that the Navy did not have the time and resources necessary to conduct those other tests and, furthermore, those tests were performed during the system component and end-to-end testing phases. In addition, nine mission-critical systems were not tested because they were not installed on the BG ships in time to participate in the U.S.S. *Constellation* BGSIT. Also, contingency plans were tested on the BGSIT only for those systems that failed to operate during the Y2K rollover test.

Objectives

The overall audit objective was to evaluate whether the Space and Naval Warfare Systems Command effectively prepared for the U.S.S. *Constellation* BGSIT for the Y2K impact and to make recommendations for improving future BGSITs. The audit focused on the Space and Naval Warfare Systems Command mission-critical systems that required a Y2K renovation to be installed on ships in the U.S.S. *Constellation* BG. Specifically, we reviewed initialization procedures, contingency plans, and the planning and installing of Y2K renovations for the U.S.S. *Constellation* BGSIT. See Appendix A for a discussion of the scope, methodology, and prior audit coverage.

A. Year 2000 Initialization Procedures for Vulnerable Systems

SPAWAR program managers did not thoroughly prepare and review initialization procedures to ensure that they included the steps for system operators to follow in conducting Y2K tests and to back up and recover system data. Initialization procedures were inadequate because SPAWAR program managers did not have an effective process to ensure that they met all initialization procedure requirements. As a result, test managers may not have effective initialization procedures to validate systems in a Y2K environment during future BGSITs.

Purpose of Initialization Procedures

Initialization procedures provide system operators with steps to advance the system clock and then roll back the clock to its prior date. Implementation of the initialization procedures allows the system operators to validate the system capability to operate in the year 2000 and beyond. Initialization procedures were designed as stand-alone procedures for each vulnerable system and were the starting point for developing the test plan for the U.S.S. *Constellation* BGSIT Final Integration Testing. Initialization procedures are required to address date initialization, data recording, and system restoration. During the U.S.S. *Constellation* BGSIT, system operators used initialization procedures to roll over the system date, to record specific data points and observations, and to restore the system to the correct date.

SPAWAR Vulnerable Systems

The Navy defined Y2K vulnerable systems as systems (hardware, software, or firmware) that use date information provided by an external source (including operator entry) or generated by an internal source for internal use or export. Therefore, any system or system component that has a date associated with its input or output is vulnerable. The U.S.S. *Constellation* BG had 74 SPAWAR vulnerable systems. Y2K vulnerable systems (mission critical or mission support) require initialization procedures. The SPAWAR program managers are responsible for preparing initialization procedures for each vulnerable system that they manage.

Initialization Procedure Process

The Chief of Naval Operations designated the Naval Sea Systems Command as the lead Systems Command (SYSCOM) for Y2K testing. In that role, the Naval Sea Systems Command was responsible for developing the guidelines and

procedures for other SYSCOMs to use in preparing initialization procedures. The Naval Sea Systems Command assigned the Dahlgren Division, Naval Surface Warfare Center, to act as a repository for initialization procedures, to review the format of initialization procedures and to forward the initialization procedures to the Fleet Commanders for use in the U.S.S. *Constellation* Y2K BGSIT. The SYSCOMs were responsible for preparing the initialization procedures and for reviewing the content of the initialization procedures for all vulnerable systems that are installed on Navy ships and aircraft and those shore systems directly linked to the fleet.

SPAWAR Initialization Procedure Status

The SPAWAR initialization procedures did not always address the actual steps that system operators were to follow in advancing the system clock and in restoring the data when the clock was restored to its prior date. Program managers were to complete initialization procedures by December 18, 1998. As of January 11, 1999, SPAWAR submitted 42 of 74 initialization procedures to the Naval Sea Systems Command for review. The Naval Sea Systems Command returned 26 initialization procedures to SPAWAR because the procedures did not address the extraction point for recording Y2K pertinent data. For example, the Global Command and Control System-Maritime Afloat initialization procedures did not include data recording elements or identify the initialization procedure for the equipment.

The Commander-in-Chief, U.S. Pacific Fleet, Y2K Office sponsored an Operational Validation Readiness Review from January 6 through 9, 1999. This review changed the initialization procedure requirements and extended the due date to January 22, 1999. The SYSCOMs were requested to revise their initialization procedures to include the names and telephone numbers of the program and technical managers responsible for the system, provide instructions for advancing the system clock for testing, and provide step-by-step procedures for both the backup data and restoration processes. For those systems in which the Commander-in-Chief, U.S. Pacific Fleet, Y2K Office did not receive suitable initialization procedures, the responsible SYSCOM was required to provide a subject matter expert to execute the initialization procedure in the BGSIT for each ship with that system installed.

The Commander-in-Chief, U.S. Pacific Fleet, Y2K Office obtained some revised initialization procedures from the Dahlgren Division, Naval Surface Warfare Center, for the systems that were to be validated during the U.S.S. *Constellation* BGSIT. Two weeks before the U.S.S. *Constellation* BGSIT, we reviewed those revised initialization procedures and determined that the procedures met the Operational Validation and Readiness Review criteria. However, the Commander-in-Chief, U.S. Pacific Fleet, Y2K Office had not received all revised initialization procedures at the time of our review. As a result, several systems had last minute changes to their initialization procedures and the changes were not processed through the initialization procedure repository and provided to the Commander-in-Chief, U.S. Pacific Fleet, Y2K Office in final form for the Operational Validation Readiness Review.

Recommendation and Management Comments

A. We recommend that the Commander, Space and Naval Warfare Systems Command, develop an effective review process for initialization procedures. The review process should require program managers to thoroughly evaluate initialization procedures before forwarding them to the system operators. The process should require the return of those initialization procedures for future Battle Group Systems Integration Tests that do not include step-by-step procedures to adjust the system date and restore and recover lost data to the program manager for revision.

Management Comments. The Navy concurred and stated that the Y2K Office implemented a step-by-step quality assurance review process to determine the adequacy of initialization procedures. The quality assurance review process assigns responsibility to the Y2K Office for evaluating and approving initialization procedures before sending them to the fleet for system operator use. The Y2K Office will return those initialization procedures that do not pass the quality assurance review to the responsible program manager for revision.

B. Contingency Planning

The SPAWAR contingency plans generally did not provide ship personnel with specific contingency procedures to follow in the event of system degradation or complete system failure because of a Y2K problem. The plans did not have complete contingency procedures because SPAWAR program managers did not always follow the Navy Y2K Project Office contingency plan guidance. In addition, SPAWAR did not develop an effective quality assurance process to review the completeness of contingency plans. Properly prepared contingency plans are essential to maintain mission capability, to restore systems to full operational capability efficiently and effectively, and to provide the ship force with contingency actions that are well defined, documented, tested, and feasible.

Scope and Criteria

We identified 19 mission-critical systems that required a Y2K renovation to be installed on ships in the U.S.S. *Constellation* BG. Program managers prepared contingency plans for 18 of those systems, and one program manager did not prepare a contingency plan for the Contingency Theater Automated Planning System. We used the Navy Y2K Project Office guidance, "Navy Y2K Contingency and Continuity-of-Operations Planning Guide," November 1, 1998, as the criteria for evaluating the adequacy of the SPAWAR prepared contingency plans. The BGSIT Y2K test plan did not make provisions for testing contingency plans unless a system encountered a Y2K failure during rollover testing.

SPAWAR Contingency Plan Guidance

Navy Contingency Plan Guidance. Appendix A of the Navy Y2K contingency plan guidance discusses five elements (preparation, planning, overview, execution, and recovery) required in contingency plans for mission-critical systems. We focused on the first three elements because the last two pertain to the execution phase that begins when a contingency situation occurs.

Preparation Elements. The Navy Y2K contingency plan guidance states that the primary purpose of the preparation element is to ensure that contingency actions are well defined, documented, and feasible. Included in the preparation elements are system failure solutions, workarounds, and procedures to do the following:

- recognize degradation of system functions and judge the results;
- detect possible corrupt data within the system;

-
- report system failure to system owners with points of contact and phone numbers; and
 - perform workarounds and preserve, protect, and recover lost or damaged data.

Of 18 SPAWAR contingency plans for mission-critical systems reviewed, 10 plans did not include methods for one or more of the following preparation elements: identifying the degradation of a system, detecting corrupt data, developing workarounds, or recovering data.

Planning Elements. The Navy Y2K contingency plan guidance states that the primary purpose of the planning elements is to identify potential risks and develop strategies for handling those risks. Specifically, the planning elements should do the following:

- identify possible risks and assess the likelihood, impact, and priority of each risk;
- identify alternative strategies to minimize the operational impacts of each risk; and
- describe and quantify the system and mission impacts of each identified risk.

Of 18 SPAWAR contingency plans for mission-critical systems, 8 plans did not describe the mission impact of each identified risk, and 4 of those 8 contingency plans also did not identify alternative strategies to minimize the operational impacts of each risk.

Overview Elements. The Navy Y2K contingency plan guidance addresses the following three key overview elements: plan validation and testing; roles, responsibilities, and authority; and system description.

Program offices should test and validate systems regularly and modify contingency plans to reflect changes needed to correct deficiencies discovered during testing. The plans should identify the roles, responsibilities, and authority of program managers, system managers, system customers, and appropriate points of contact for each organization. The SYSCOM should provide a system description that identifies all software, devices, and components satisfying the system functional requirements. Also, SYSCOMs should identify all system interfaces, provide a brief statement of the function(s) performed by a system, describe the criticality of the system, and include the potential impact that the loss or degradation of the system would have on a unit or the battle group mission. Of 18 SPAWAR contingency plans, 5 plans did not meet the overview criteria.

Results of SPAWAR Contingency Plans Review

Our review of 19 systems showed that a contingency plan was not prepared for 1 system (Contingency Theater Automated Planning System), and contingency plans for 10 of the systems did not meet the Navy Y2K contingency plan guidance.

The following table provides a summary of SPAWAR Y2K contingency plan deficiencies (noted by an X) by preparation, planning, and overview elements. The narrative of each system's deficiencies follows the table.

Summary of SPAWAR Y2K Contingency Plan Deficiencies

System	Preparation Elements				Planning Elements		
	Identified Degradation Of System	Detect Corrupt Data	Work-Arounds	Recovery of Data	Risks, Potential Impacts, and Priority	Alternative Strategies	Overview Elements
CHBDL-ST		X			X		
COBLU 0	X	X	X	X	X	X	X
EHF LDR	X	X	X				
GCCS-M	X	X		X			
HFRG	X	X	X	X	X	X	X
NAVMACS II	X	X	X		X		X
NECC	X	X	X	X	X	X	X
SCI-ADNS	X	X	X		X		X
SSEE Phase II		X			X		
TRE	X	X	X	X	X	X	
CHBDL-ST	Common High Bandwidth Data Link Surface Terminal						
COBLU 0	Cooperative Outboard Logistics Update, Phase 0						
EHF LDR	Extremely High Frequency Low Data Rate						
GCCS-M	Global Command and Control System-Maritime Afloat						
HFRG	High-Frequency Radio Group						
NAVMACS II	Naval Modular Automated Communications System II						
NECC	Navy Extremely High Frequency Communications Controller						
SCI-ADNS	Sensitive Compartmented Information-Automated Digital Network System						
SSEE Phase II	Ships Signal Exploitation Equipment Phase II						
TRE	Tactical Receive Equipment						

Common High Bandwidth Data Link Surface Terminal. The Common High Bandwidth Data Link Surface Terminal system supports high data rate communications between surface and airborne systems. The contingency plan did not fully meet the Navy criteria in the preparation and planning elements.

Preparation Elements. The contingency plan did not provide procedures to detect and correct corrupt data.

Planning Elements. The contingency plan did not describe the mission impact of each identified risk.

Cooperative Outboard Logistics Update. The Cooperative Outboard Logistics Update system is an upgrade that modernizes the existing countermeasures exploitation system. The contingency plan did not fully meet the Navy criteria in the preparation, planning, and overview elements.

Preparation Elements. The Cooperative Outboard Logistics Update contingency plan did not contain workaround procedures. The contingency plan stated that if the contingency mode were implemented then the program manager would take action to either correct the problem or develop workaround procedures. However, one of the purposes of the contingency plan is to have workaround procedures available to ship personnel in the event of a Y2K-induced system failure. The contingency plan also did not address procedures to recognize degradation of system functions or to detect possible corrupt data within the system. In addition, the contingency plan did not provide procedures to recover data. The Navy criteria state that procedures for recovering lost or damaged data should define or reference the documented actions and associated procedures necessary for recovering lost or damaged data. The Navy criteria also state that documented procedures should be there to preserve and protect system data.

Planning Elements. The Cooperative Outboard Logistics Update contingency plan did not address alternative strategies and did not describe the mission impact of each identified risk.

Overview Elements. The Cooperative Outboard Logistics Update contingency plan addressed the system Y2K testing effort and not the contingency plan validation effort. In addition, the contingency plan did not provide a point of contact for each of the three organizations identified in the roles, responsibilities, and authority element. Finally, the contingency plan did not include in the system description the system interfaces and the potential impact that the loss or degradation of the system would have on a unit or the battle group mission.

Extremely High Frequency Low Data Rate. The Extremely High Frequency Low Data Rate system is the Navy satellite communications program designed to accommodate a wide variety of command and control communications applications (that is, secure voice, teletype, data, and fleet broadcast systems). The contingency plan did not fully meet the Navy Y2K contingency plan criteria for the preparation element. The contingency plan did not provide workaround procedures. Instead, it referred ship personnel to the continuity-of-operations plan (COOP). In addition, the contingency plan did not provide procedures to identify degradation of the system or procedures to detect corrupt data.

Global Command and Control System-Maritime Afloat. The Global Command and Control System-Maritime Afloat system provides a single command, control, communications, computer, and intelligence capability to sea-based forces. The contingency plan did not fully meet the Navy Y2K

contingency plan guidance requirements for the preparation element. For example, the contingency plan did not provide detailed procedures to identify degradation of the system, detect corrupt data, and recover data.

High-Frequency Radio Group. The High-Frequency Radio Group system provides both high-frequency broadband and high-frequency narrowband configurations. The system replaces existing high-frequency equipment on ships with a requirement for 10 or more high-frequency transmitters. The system contingency plan did not meet the Navy Y2K contingency plan criteria for the preparation, planning, and overview elements.

Preparation Elements. The contingency plan did not contain procedures to identify degradation of the system or detect corrupt data. In addition, the contingency plan did not address a workaround or provide data recovery procedures.

Planning Elements. The contingency plan did not address alternative strategies and did not describe the mission impact of each identified risk.

Overview Elements. The contingency plan did not properly address the plan validation and testing element. The contingency plan did not state whether it had been validated and tested or how the plan would be maintained and updated. In addition, the contingency plan did not provide the ship personnel with a point of contact in the event that the system encountered a Y2K problem. The contingency plan also did not provide the potential impact that the loss or degradation of the system would have on a unit or the battle group mission. Finally, the contingency plan did not provide a description of the system, including its mission functions and interfaces.

Naval Modular Automated Communications System II. The Naval Modular Automated Communications System II is an automated messaging handling system that receives, processes, stores, and distributes message traffic. The contingency plan did not fully meet the Navy Y2K contingency plan criteria in the preparation, planning, and overview elements.

Preparation Elements. The contingency plan did not provide for workaround procedures and referred users to COOPs while SPAWAR program managers developed workarounds and system corrections. Also, the contingency plan did not provide specific procedures to recognize degradation of system functions or to detect possible corrupt data within the system.

Planning Elements. The contingency plan did not provide a description of the mission impact of each identified risk.

Overview Elements. The contingency plan did not provide the potential impact that the loss or degradation of the system would have on a unit or the battle group mission and did not adequately address the contingency plan validation and testing effort. The contingency plan stated that the plan might be invoked as part of the shipboard end-to-end testing accomplished Navywide, but did not state how the contingency plan would be validated and tested if this plan was not invoked during the end-to-end testing.

Navy Extremely High Frequency Communications Controller. The Navy Extremely High Frequency Communications Controller system is a planned product improvement to the Navy satellite program terminal providing information exchange system services over satellite communications. The contingency plan did not fully meet the Navy Y2K contingency plan criteria for the preparation, planning, and overview elements.

Preparation Elements. The contingency plan did not document any workaround procedures, but instead referred ship personnel to COOPs. In addition, the contingency plan did not provide procedures to identify degradation of the system, detect corrupt data, or recover data.

Planning Elements. The contingency plan did not describe the mission impact of each identified risk and did not provide any alternative strategies. The contingency plan stated that the system had no real operational risk.

Overview Elements. The contingency plan did not provide a description of the system including its mission and functions and information on system interfaces.

Sensitive Compartmented Information-Automated Digital Network System. The Sensitive Compartmented Information-Automated Digital Network System is a follow-on initiative within the Tactical Intelligence Information Exchange Subsystem Program. The Tactical Intelligence Information Exchange Subsystem Program provides real-time and near real-time tactical cryptologic support to afloat commanders. One of the primary benefits of the Sensitive Compartmented Information-Automated Digital Network System is the use of all portions of the available radio frequency spectrum for network communications. The contingency plan did not fully meet the Navy Y2K contingency plan criteria in the preparation, planning, and overview elements.

Preparation Elements. The contingency plan did not provide for workaround procedures. The contingency plan stated that users should refer to the COOP while the program office develops workarounds and system corrections. The COOP is written by functional warfare mission area (that is, anti-submarine warfare) and would not provide information on how to get the system operational. Workaround procedures should be available to the ship personnel before a system failure or degradation caused by a Y2K problem. Also, the contingency plan did not provide specific procedures to recognize degradation of system functions or to detect possible corrupt data within the system.

Planning Elements. The contingency plan did not provide a description of the mission impact of each identified risk.

Overview Elements. The contingency plan did not provide the potential impact the loss or degradation of the system would have on a unit or the battle group mission and did not provide a description of the interfaces of the system.

Ships Signal Exploitation Equipment Phase II. The Ships Signal Exploitation Equipment Phase II program is a signal exploitation system that allows the

operators to monitor and analyze signals within the ship and aboard different ship classes. The contingency plan did not fully meet the Navy Y2K contingency plan criteria in the preparation and planning elements.

Preparation Elements. The contingency plan did not have procedures to detect and correct corrupt data.

Planning Elements. The contingency plan did not describe the mission impact of each identified risk.

AN/USQ-101 (V) Tactical Receive Equipment. The AN/USQ-101 (V) Tactical Receive Equipment system is a suite of tactical receiving equipment used to receive broadcasts. The system has four major components; however, the contingency plan was written for only the message processor and not the remaining three components. Also, the contingency plan did not fully meet the Navy Y2K contingency plan guidance for the preparation and planning elements.

Preparation Elements. The contingency plan did not document workaround procedures and did not provide procedures to identify degradation of the system, detect corrupt data, or recover data.

Planning Elements. The contingency plan did not describe and quantify the mission impact of each identified risk and is not clear on alternative strategies. The contingency plan states that the message processor has no operational replacement, but then it lists possible replacements, and, furthermore, the plan makes it incumbent on the system user to identify a secondary source.

Contingency Theater Automated Planning System. The Contingency Theater Automated Planning System is an Air Force developed and designed theater-level air mission planning system. The Joint Chiefs of Staff designated it the joint system responsible for the production and dissemination of air tasking orders, which are United States military text format messages. The program manager believed that she was not required to prepare a contingency plan because the Contingency Theater Automated Planning System was to be replaced by the Air Force's Theater Battle Management Core System prior to the year 2000. However, our position was that because the Theater Battle Management Core System could be delayed in development, a contingency plan should be prepared for the Contingency Theater Automated Planning System. Additionally, the Department of the Navy Year 2000 Action Plan requires contingency plans by December 31, 1998, for all mission-critical systems. We were informed after our audit field work was completed that the Theater Battle Management Core System would be delayed and that the Contingency Theater Automated Planning System would be renovated and require a contingency plan.

Quality Assurance Reviews

Program offices were not performing adequate quality assurance reviews of contingency plans to ensure that they met the requirements of the Navy Y2K contingency plan guidance, which became evident when SPAWAR made the decision to use a contractor to conduct quality assurance reviews on contingency plans.

Summary

The SPAWAR contingency plans did not always provide contingency actions that were well defined, documented, and useful to the system operator. Contingency plans referred ship personnel to the COOPs; however, COOPs did not provide sufficient information on bringing the system back to its operational capability. In addition, SPAWAR contingency plans generally did not describe the mission impact of each identified risk and did not fully meet the overview criteria. Program managers did not always perform adequate quality assurance reviews of contingency plans before the plans were sent to the Type and Fleet Commanders for review and feedback. Contingency planning is essential to maintaining mission capability and to restoring systems to full operational capability efficiently and effectively. Also, for devices with embedded microprocessors that are difficult to identify and test for Y2K compliance, contingency planning may be the only effective method of mitigating potential mission degradation.

Recommendations and Management Comments

B.1. We recommend that the Commander, Space and Naval Warfare Systems Command, develop a more effective quality assurance process to review the completeness of all contingency plans in accordance with the Navy Year 2000 Project Office contingency plan guidance. Those contingency plans that do not include well defined and documented contingency actions, step-by-step solutions, and workarounds should be returned to the program managers with instructions to revise the plans to address Navy contingency plan requirements.

Management Comments. The Navy concurred and stated that the Y2K Office implemented a stringent contingency plan review process for evaluating the adequacy of contingency plans before sending them to the fleet for system operator use. The Y2K Office also disseminated Navy and DoD contingency plan guidance and a contingency plan development template to assist program managers in preparing contingency plans. Program managers will revise previously identified deficient contingency plans by June 15, 1999, and will complete the remaining contingency plans by July 1, 1999.

B.2. We recommend 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.

Management Comments. The Navy concurred and stated that initialization procedures and a contingency plan will be completed after the new Contingency Theater Automated Planning System completes certification testing in June 1999. Estimated completion of the recommended action is August 1999.

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 list of audit projects addressing the issue, see the Y2K webpage on IGnet at <http://www.ignet.gov>.

Scope

Work Performed. We reviewed DoD and Navy guidance on Y2K test and contingency plans, continuity-of-operations plans, initialization procedures, and installation procedures for Y2K renovations. We interviewed key Navy officials from various commands including the Navy Y2K Program Office, Systems Commands, and the Operational Forces on the management approach for implementing Y2K programs and initiatives. We evaluated the Space and Naval Warfare Systems Command's contingency plans for mission-critical systems that were to be installed on ships in the U.S.S. *Constellation* Battle Group to correct a Y2K problem. We also evaluated the installation planning and scheduling process, the continuity-of-operations process, and the initialization procedure process.

DoD-Wide Corporate-Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, the Department of Defense has established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting the objectives. This report pertains to achievement of the following objective and goal.

Objective: Prepare now for the uncertain future. **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. (DoD-3)

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objective and goal:

Information Technology Management Functional Area.

Objective: Provide services that satisfy customer information needs.

Goal: Upgrade technology base. (ITM-2.3)

General Accounting Office High-Risk Area. The General Accounting Office has identified the resolution of the Y2K conversion problem as one of several high-risk areas in DoD. This report provides coverage of that problem of the overall Information Management and Technology high-risk area.

Methodology

Use of Computer-Processed Data. We did not use computer-processed data or statistical sampling procedures for this audit. However, we evaluated Y2K documents dated from June 1995 through January 1999 and evaluated various Navy Y2K databases used to plan, execute, and coordinate the Navy Y2K effort.

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from November 1998 through January 1999, in accordance with the auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD.

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

Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at <http://www.gao.gov>. Inspector General, DoD, reports can be accessed over the Internet at <http://www.dodig.osd.mil>.

Appendix B. Other Matters of Interest

SPAWAR Y2K War Room

The SPAWAR effort in establishing a Y2K War Room is commendable. SPAWAR management recognized the fast-paced transcending Y2K issues and the coordination required across a broad spectrum of organizations to resolve Y2K issues. SPAWAR established the war room in September 1998, to provide a collaborative environment in which to coordinate and monitor system-wide Y2K problems and solutions. Daily activities in the war room include status meetings; document reviews; data calls; DoD, Department of the Navy, and fleet responses; and planning and scheduling conferences. The war room also provides SPAWAR with the capability to coordinate end-to-end testing and to support other Navy Y2K tests. The war room capabilities include:

- advanced teleconferencing and video conferencing capabilities;
- extensive connectivity to other military commands, the fleet, and contractors;
- advanced systems engineering and testing stations; and
- secure communications processing and storage.

SPAWAR Y2K Timeline Summary

SPAWAR developed a comprehensive and informative timeline summary to track and monitor Y2K program management efforts. The timeline summary tracks the following information for all SPAWAR systems requiring a Y2K renovation:

- mission criticality,
- system vulnerability,
- the program office responsible,
- installation start and completion dates (actual or estimated), and
- the status of the installation.

The timeline summary tracks the information for all ships and submarines in the U.S.S. *Constellation* BG. The timeline summary is updated on a daily basis and published on a weekly basis.

Battle Group Y2K Installations

The system installation process was designed to provide a systematic planning process for installing systems stemming from developing technologies on board ships. System installation is accomplished through quarterly scheduling conferences in which proposed installations are coordinated with the Type Commanders. The Type Commanders used existing installation procedures to prioritize the installation of Y2K renovations on the U.S.S. *Constellation* BG ships.

SPAWAR did not have a central office responsible for coordinating and installing Y2K renovations until July 1998. The SPAWAR Afloat Installation Manager Office was established at that time to develop and maintain a ship scheduling and installation facilitation process.

SPAWAR Program Offices manage 23 mission-critical systems requiring Y2K renovation and installation on U.S.S. *Constellation* BG ships. Nine of those mission-critical systems were not installed on U.S.S. *Constellation* BG ships before the BGSIT. In addition, one mission-critical system, requiring Y2K renovation and installation, did not have an estimated or actual completion date. SPAWAR should have estimated or actual dates for those systems so that Y2K testing can be accomplished during future BGSITs. The U.S.S. *John F. Kennedy* is the next BG scheduled for a Y2K BGSIT in late May 1999.

Appendix C. Report Distribution

Office of the Secretary of Defense

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

Joint Staff

Director, Joint Staff

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Commander-in-Chief, U.S. Pacific Fleet
Commander-in-Chief, U.S. Atlantic Fleet
Chief Information Officer, Department of the Navy
Navy Year 2000 Project Office
Commander, Third Fleet
Commander, Naval Air Force, U.S. Pacific Fleet
Commander, Naval Surface Force, U.S. Pacific Fleet
Commander, Space and Naval Warfare Systems Command
Inspector General, Department of the Navy
Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
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 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

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

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

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

Department of the Navy Comments



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

18 May 99

MEMORANDUM FOR THE DEPARTMENT OF DEFENSE ASSISTANT INSPECTOR
GENERAL FOR AUDITING

Subj: AUDIT REPORT ON SPACE AND NAVAL WARFARE SYSTEMS COMMAND
PREPARATIONS FOR BATTLE GROUP SYSTEMS INTEGRATION TESTING
(PROJECT NO. 9AD-0078)

Ref: (a) DODIG memo of 22 Apr 99

Encl: (1) Department of the Navy Response to Draft Audit Report

I am responding to the draft audit report forwarded by reference (a) concerning Year 2000 Space and Naval Warfare Systems Command preparations for battle group systems integration testing (PROJECT NO. 9AD-0078)

One of the Department of the Navy's highest priorities is to ensure no mission critical system failures occur due to Year 2000 (Y2K) related problems. To address this issue, the Department has provided guidance which outlines a centralized management/ decentralized execution policy. The Department's Y2K progress is reported to Senior Management during regularly scheduled briefings. These reports examine Echelon II Commands for proper allocation of resources, for progress against Department of the Navy and Department of Defense mandated milestones, for contingency plans, for responsibility assignment and identification of system interfaces, for required Memoranda of Agreement, and for use of the Department of the Navy Y2K Database.

The Department of the Navy's response is provided at enclosure (1). We concur with the finding and recommendations in the draft report. The Commander, Space and Naval Warfare Systems Command take his Y2K responsibilities seriously and has taken appropriate steps to ensure that the conduct of the Command's mission will not be adversely affected by Y2K induced failures.

Subj: AUDIT REPORT ON SPACE AND NAVAL WARFARE SYSTEMS COMMAND
PREPARATIONS FOR BATTLE GROUP SYSTEMS INTEGRATION TESTING
(PROJECT NO. 9AD-0078)

Your findings and recommendations have been helpful in identifying necessary changes in our approach to solving this very important challenge. My point of contact is Ms. Mahnaz Dean, (703) 602-6280.



D. M. Wennergren
Deputy for Y2K and
Information Assurance

Copy to:
CMC
CNO
UNSECNAV
ASSTSECNAV RD&A
CINCPACFLT
Naval Inspector General
Inspector General Marine Corps
Naval Audit Service
USMC CIO
USN Y2K Project Office
NAVINGEN(02)
ASSTSECNAV FM&C (FMO-31)
COMSPAWARSYSCOM

Space and Naval Warfare Systems Command (SPAWAR)
Responses to
DODIG Audit Report #9AD-0078
Space and Naval Warfare Systems Command Preparation for Battle Group Systems
Integration Testing

Recommendation A: "We recommend that the Commander, Space and Naval Warfare Systems Command, develop an effective review process for initialization procedures. The review process should require program managers to thoroughly evaluate initialization procedures before forwarding them to the system operators. The process should require the return of those initialization procedures for future Battle Group Systems Integration Tests that do not include step-by-step procedures to adjust the system date and restore and recover lost data to the program manager for revision."

Response: Concur. A quality review process is now in place and is pictorially represented in Diagram 1. Positive feedback regarding Initialization Procedure (IP) quality has been received from the IP Coordinator, Naval Sea Systems Command (NAVSEA). Feedback on potential improvements is evaluated and incorporated upon receipt.

IPs for remaining systems in implementation will be submitted for review to SPAWAR OSC by 14 May 1999.

Process Flow for Initialization Procedure
Review and Web Publication

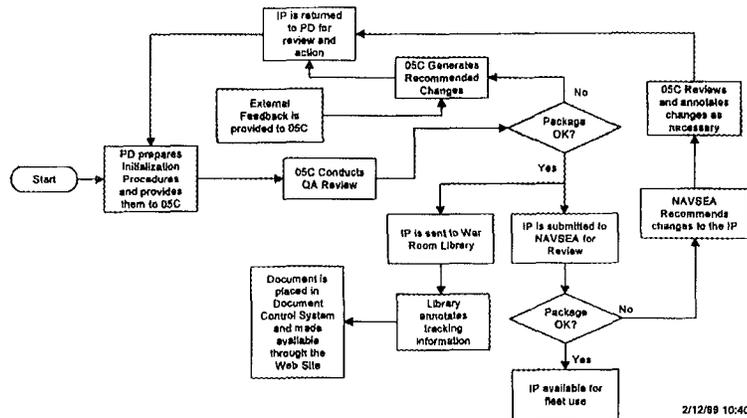


Diagram 1

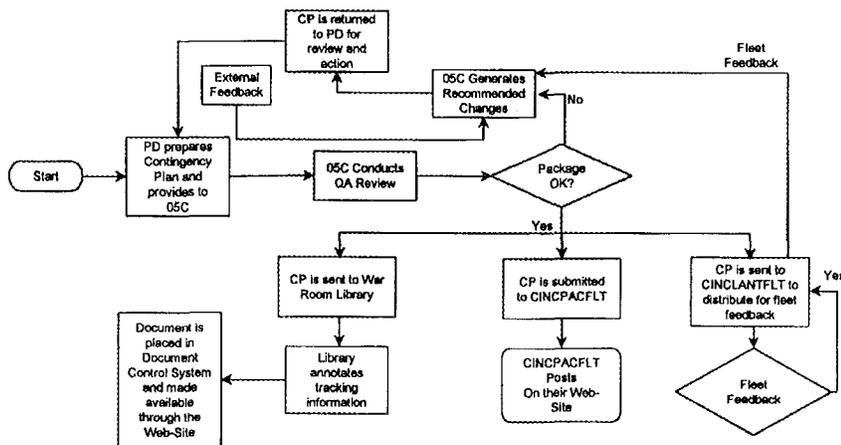
Enclosure (1)

Recommendation B1: “We recommend that the Commander, Space and Naval Warfare Systems Command, develop a more effective quality assurance process to review the completeness of all contingency plans in accordance with the Navy Year 2000 Project Office contingency plan guidance. Those contingency plans that do not include well defined and documented contingency actions, step-by-step solutions, and workarounds should be returned to the program managers with instructions to revise the plans to address Navy contingency plan requirements.”

Response: Concur. A stringent quality review process is now in place and is pictorially represented in Diagram 2. Additionally, a Contingency Plan (CP) guideline that incorporates DoN Chief Information Office (CIO) Year 2000 (Y2K) Action Plan, Navy Y2K Contingency and Continuity of Operations Planning Guide, and DODIG guidance has been disseminated to assist the Program Managers in the development of their CPs. This guide, SPAWAR Contingency Plan Development Template of 21 April 1999, is now featured on the DoN CIO Y2K Home Page as the standard template for CP development.

The deficient CPs reviewed in the audit will be completed prior to 15 June 1999 and all others will be completed by 1 July 1999.

Process Flow for Contingency Plan Review and Web Publication



2/12/99 10:46

Diagram 2

Recommendation B.2: “We recommend 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.”

Response: Concur. SPAWAR PMW-157 is the Navy Program Office responsible for the fielding of CTAPS within the Navy. The currently operationally fielded version of CTAPS, Version 5.2.2, is not Y2K compliant. Version 5.2.3, which will be Y2K compliant, is under development and is scheduled to complete certification testing in June 1999. PMW-157 will have an IP and CP ready when certification is complete. This system IP and CP will undergo the existing review processes. Estimated completion date is August 1999.

Audit Team Members

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

Thomas F. Gimble
Patricia A. Brannin
Robert K. West
Robert W. Otten
Jerel B. Silver
Marvin E. Tuxhorn
Benedicto M. Dichoso
Kathryn J. Ross