Audit Report

YEAR 2000 CONTINGENCY PLANS FOR SURFACE SHIP HULL, MECHANICAL, AND ELECTRICAL SYSTEMS

Report Number 99-170 May 24, 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

HM&E	Hull, Mechanical, and Electrical
NAVSSES	Naval Ship Systems Engineering Station
Y2K	Year 2000

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

May 24, 1999

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

SUBJECT: Audit Report on Year 2000 Contingency Plans for Surface Ship Hull, Mechanical, and Electrical Systems (Report No. 99-170)

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 the requirements of 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.

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-170 **May 24, 1999**
(Project No. 8AD-0053.00)

Year 2000 Contingency Plans for Surface Ship Hull, Mechanical, and Electrical Systems

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.

Objectives. The overall audit objective was to evaluate year 2000 conversion actions that the Navy took for surface ship hull, mechanical, and electrical systems. Specifically, we reviewed year 2000 certification tests, contingency plans, and initialization procedures.

Results. The Integrated Information Systems Engineering Group, Naval Sea Systems Command, implemented a year 2000 certification test checklist and prepared initialization procedures for system operators to use in the year 2000 rollover (Appendix B). However, the contingency plans prepared for hull, mechanical, and electrical systems did not properly address the key elements in the Navy year 2000 contingency plan guidance. See the Finding section for details.

Summary of Recommendations. We recommend that the Director, Integrated Information Systems Group, Naval Sea Systems Command, develop a more effective quality review process and revise the hull, mechanical, and electrical contingency plans that did not meet the Navy year 2000 planning guidance.

Management Comments. The Navy concurred with the recommendations. The Integrated Information Systems Group has strengthened its quality assurance review process and revised its hull, mechanical, and electrical systems contingency plans. See the Finding section for a discussion of management comments and the Management Comments section for the complete text of the comments.

Table of Contents

Executive Summary i

Introduction

Background 1
Objectives 2
Contingency Plans for Surface Ship Hull, Mechanical, and Electrical Systems 3

Appendixes

A. Audit Process
Scope 12
Methodology 12
Summary of Prior Coverage 13
B. Other Matters of Interest 14
C. Report Distribution 15

Management Comments

Department of the Navy Comments 17

Background

The year 2000 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 next century.

Because of the 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 year 2000 (Y2K) problem and that the head of each agency ensure that efforts to address the Y2K problem receive the highest priority attention of the agency.

DoD Y2K Management Plan. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued the "DoD Year 2000 Management Plan" in April 1997. The latest version was released in January 1999. The DoD Y2K Management Plan provides the overall DoD strategy and guidance for inventorying, prioritizing, repairing or retiring systems, and monitoring Y2K progress. The DoD Y2K 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 revised its action plan in September 1998 to outline the Navy Y2K management strategy; provide Y2K guidance; define roles, responsibilities, and reporting requirements; and lay a foundation to ensure that no mission-critical failure occurs because of Y2K-related problems.

Navy Y2K Contingency and Continuity-of-Operations Planning Guide. The Navy Y2K Project Office issued the "Navy Y2K Contingency and Continuity-of-Operations Planning Guide" on November 1, 1998, to help ensure that the Navy would not lose any of its mission capability because of a Y2K problem.

Navy Technical Authority. The Naval Sea Systems Command is the Navy technical authority for ships and ship systems. The Naval Sea Systems Command Chief Engineer, Deputy Commander for Engineering, is responsible for exercising technical authority, establishing technical policy and standards, and enforcing their compliance.

Y2K Point of Contact. On August 21, 1998, the Naval Sea Systems Command Chief Engineer, Deputy Commander for Engineering, designated the Integrated Information Systems Engineering Group as the point of contact for all Y2K issues within the Naval Sea Systems Command Engineering Directorate. As the Y2K point of contact, the group is responsible for representing the Naval Sea Systems Command Engineering Directorate on all Y2K issues concerning ship hull, mechanical, and electrical (HM&E) systems. The group appointed an HM&E Y2K point of contact to monitor the Y2K conversion of HM&E systems.

HM&E Systems. Approximately 252 HM&E systems are installed on Navy surface ships. Included in those systems are "dumb" iron and nonelectronic parts, which do not have a Y2K vulnerability, as well as other items that contain data processors and may therefore be vulnerable. The Naval Sea Systems Command Y2K Project Office identified 14 mission-critical HM&E systems for Y2K reporting. Those 14 systems have been certified as Y2K compliant.

Objectives

The overall audit objective was to determine whether the Integrated Information Systems Engineering Group effectively implemented Navy Y2K guidance in the conversion of surface ship HM&E systems. Specifically, we reviewed Naval Sea Systems Command Y2K certification tests, contingency plans, and initialization procedures for HM&E systems. Refer to Appendix A for a discussion of the audit scope and methodology and Appendix B for a discussion of certification and initialization procedures.

Contingency Plans for Surface Ship Hull, Mechanical, and Electrical Systems

The Integrated Information Systems Engineering Group, Naval Sea Systems Command, approved contingency plans for surface ship hull, mechanical, and electrical systems that did not meet the Navy contingency plan guidance in its entirety. The contingency plans were incomplete because the Integrated Information Systems Engineering Group did not establish an effective quality assurance review process for contingency plans. As a result, system users may not have acceptable contingency procedures to follow in the event of degradation or complete failure of a mission-critical system because of a Y2K issue.

Background

Engineering Operational Sequencing System. In September 1976, the Chief of Naval Operations established the engineering operational sequencing system to provide system users with a single consolidated source of information for operating engineering and casualty control systems. The system consists of systematic, detailed written procedures using charts, instructions, and diagrams that allow the system user to transition between safe operating conditions and casualty restoration. Contingency plans supplement existing engineering operational sequencing system procedures for HM&E systems.

Naval Sea Systems Command Y2K Memorandum. On October 20, 1998, the Executive Director, Naval Sea Systems Command, issued a Y2K systems contingency planning memorandum stating that contingency plans for mission-critical systems were to provide sufficient detail to allow a system user to correct, modify, or change the system operation to fulfill its mission.

Navy Contingency Plan Guidance

Navy Contingency Planning Guide. 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 our review on the first three elements because the last two pertain to the execution phase that begins when a contingency situation occurs.

Preparation Elements. The primary purpose of the preparation elements is to ensure that contingency actions are well defined, documented, and feasible for each risk. The Navy guide suggests several procedures to consider under the preparation elements. The procedures include the following:

- recognize system degradation,
- detect possible corrupt data within the system,

- report system failure,
- preserve and protect data, and
- work around Y2K-related failures.

Planning Elements. The primary purpose of the planning elements is to identify potential risks and develop strategies for those risks. The planning elements should identify possible Y2K risks or events that may cause a contingency situation and describe the probability, system and mission impact, and priority associated with each identified risk. The planning elements should also list feasible alternative strategies that will reduce the likelihood and impact of each identified risk.

Overview Elements. The Navy planning guide established overview elements that contain information about the system and the preparation of the contingency plan. Two key overview elements are the system description and plan validation and testing. The contingency plan should provide a system description that identifies all software, devices, and components required to satisfy the system functional requirements. The contingency plan should also discuss the validation, testing, and modification of the contingency plan.

Results of HM&E Contingency Plan Review

Our review of 14 HM&E contingency plans showed that 13 of the plans did not meet the Navy Y2K contingency plan guidance. A summary of HM&E contingency plan deficiencies (noted by an X) by preparation, planning, and overview elements are shown in the chart on the following page.

Damage Control Quarters. The Damage Control Quarters system is an automated electronic control and monitoring system that uses sensors and controllers to provide ship-wide information in real time for command, control, and communication support of total ship survivability for the U.S.S. *Rushmore* (LSD-47).

Preparation Elements. The contingency plan did not address preparation elements for the failure of the programmable logic controller, the damage control quarters application, or the shipboard network. For the Microsoft NT operating system date failure risk, the contingency plan did not provide the system user with a work around or a list of procedures to follow in the event of a contingency. Instead, the contingency plan directed the system user to report the system failure to the Naval Ship Systems Engineering Station (NAVSSES) in-service engineer to determine whether the contingency plan should be invoked. Also, the contingency plan did not identify specific procedures that the system user should follow to recognize system degradation, to detect corrupt data within the system, and to preserve and protect data as a result of a Y2K system failure.

Summary of HM&E Contingency Plan Deficiencies

	Preparation Elements				Planning Elements		
System	Identified Degradation of System	Detect Corrupt Data	Work Arounds	Recovery of Data	Risks, Potential Impacts, and Priority	Alternative Strategies	Overview Elements
DCQ	X	X	X	X	X	X	
DCS*	X	X		X	X		X
IBS	X	X	X	X	X	X	X
ISCS	X	X		X	X		X
ISMS	X	X		X	X	X	X
CG-47 MCS	X	X	X	X	X		
DDG-51 MCS	X	X	X	X	X		
LSD-41 MCS	X	X	X	X	X		X
LSD-47 MCS	X	X	X	X	X	X	
MCM-1 MCS	X	X	X	X	X		
FFG-7 PCS	X	X	X	X	X		X

CG	Cruiser	ISMS	Integrated Survivability Management System
DCQ	Damage Control Quarters	ISCS	Integrated Ship Control System
DCS	Damage Control Systems	LSD	Dock Landing Ship
DDG	Destroyer	MCS	Machinery Control System
FFG	Frigate	MCM	Mine Countermeasures Ship
IBS	Integrated Bridge System	PCS	Propulsion Control System

*The summary for the DCS represents three systems.

Planning Elements. The contingency plan identified four risks. Three risks are assigned a probability of occurrence; however, the risk of a shipboard network failure is not assigned a probability of occurrence. Also, the contingency plan did not describe system and mission impacts of the four risks or list alternative strategies for each risk.

Overview Elements. The contingency plan system description adequately identified and described the system components and software requirements. The contingency plan adequately addressed contingency plan testing.

Damage Control Systems. Although the CG-47, FFG-7, and LSD-41 class ships use a similar damage control system, the in-service engineers prepared different contingency plans for each ship class. A damage control system monitors and provides centralized status and alarm indicators for selected shipboard system functions that must be evaluated in responding to emergency conditions. The three contingency plans prepared for the different ship classes contain similar errors and, therefore, are discussed together under each element.

Preparation Elements. The contingency plans recommend that the system users implement manual work arounds for each risk, implement the continuity-of-operations plan, and report system errors to the NAVSSES in-service engineers. However, the contingency plans did not identify specific procedures that the system user should use to recognize system degradation, to detect corrupt data within the system, and to preserve and protect data as a result of a Y2K system failure.

Planning Elements. The contingency plans identified risks, quantified the probability of occurrence of those risks, discussed the system impact of those risks, and listed alternative strategies for each identified risk. However, the contingency plans did not address the mission impacts of those risks.

Overview Elements. The contingency plans' system descriptions adequately identify and describe the system components and software requirements. The plan validation and testing paragraph states that if the contingency plans were not tested during Navywide end-to-end testing then NAVSSES engineers would be tasked to test the contingency plans during the third quarter of 1999. However, the plans did not identify the organization responsible for tasking the NAVSSES engineers to perform the test.

Integrated Bridge System. The Integrated Bridge System uses manual, semi-automated, and fully automated equipment to control and monitor the course, speed, and navigation of the U.S.S. *Rushmore* (LSD-47).

Preparation Elements. The contingency plan did not provide the system user with a work around or a list of procedures to follow in the event of a contingency. The contingency plan also did not identify specific procedures that the system user was to use to recognize system degradation, to detect corrupt data within the system, and to preserve and protect data as a result of a Y2K system failure. The contingency plan directed the system user to implement the continuity-of-operations plan and to report the system failure to the NAVSSES in-service engineer.

Planning Elements. Although the contingency plan identified risks and system impacts, it did not describe the mission impacts and alternative strategies of those risks.

Overview Elements. The contingency plan system description adequately identified and described the system components and software requirements. The plan validation and testing paragraph states that if the contingency plan was not tested during Navywide end-to-end testing, then the NAVSSES engineers would be tasked to test the contingency plan during the third quarter of 1999. However, the plan did not identify the organization responsible for tasking the NAVSSES engineers to perform the test.

Integrated Ship Control System. The Integrated Ship Control System controls and monitors the propulsion, electrical, and auxiliary machinery systems on MCM-1 class ships.

Preparation Elements. The contingency plan recommended that the system user implement a manual work around for each risk, implement the continuity-of-operations, and report system errors to NAVSSES in-service engineers. However, the contingency plan did not identify specific procedures that the system user should follow to recognize system degradation, to detect corrupt data within the system, and to preserve and protect data as a result of a Y2K system failure.

Planning Elements. The contingency plan identified potential risks, the system impacts, and alternative strategies. However, the contingency plan did not address the mission impacts of those risks.

Overview Elements. The contingency plan system description adequately identified and described the system components and software requirements. The plan states that validation and testing may occur during a shipboard test before the third quarter of 1999, but the plan did not discuss who is responsible for testing the contingency plan.

Integrated Survivability Management System. The Integrated Survivability Management System is an information acquisition, processing, and display system that provides command, control, and communications for damage control decision making to support total ship survivability on the DDG-51 class ships.

Preparation Elements. The contingency plan recommended that the system users implement a manual work around for each risk, implement the continuity-of-operations plan, and report system errors to the life-cycle manager. The life-cycle manager was to task NAVSSES in-service engineers to develop additional work arounds if needed. However, the contingency plan also did not address shipboard procedures to recognize system degradation, to detect corrupt data, and to preserve and protect data as a result of a Y2K system failure.

Planning Elements. The contingency plan identified risks and addressed the system impacts of those risks. However, the contingency plan did not address mission impacts and alternative strategies for those risks.

Overview Elements. The contingency plan system description adequately identified and described the system components and software requirements. The plan states that validation and testing may occur during Navywide end-to-end testing, but it does not address when the contingency plan was to be tested and who was responsible for testing the contingency plan.

CG-47 Class Ship Machinery Control System. The Machinery Control System for the CG-47 class ship is an automated electronic control and monitoring system that controls the propulsion and electric plants and supports the auxiliary equipment.

Preparation Elements. The contingency plan provided the system user with a work around for 12 of the 18 identified risks. Also, the contingency plan directed the system user to implement the continuity-of-operations plan and

to report the system failure to the NAVSSES in-service engineer in the event of a Y2K system failure. However, the contingency plan did not identify specific procedures that the system user was to follow to recognize system degradation, to detect corrupt data within the system, and to preserve and protect data as a result of a Y2K system failure.

Planning Elements. The plan identified the risks, the system impacts, and the alternative strategies related to those risks; however, the contingency plan did not address the mission impacts of those risks.

Overview Elements. The plan system description adequately identified and described the system's components and software requirements. The plan addressed when the contingency plan would be tested and the organization responsible for the contingency plan testing.

DDG-51 Class Ship Machinery Control System. The Machinery Control System for the DDG-51 Class Ship monitors and controls the propulsion electrical, auxiliary, and damage control systems.

Preparation Elements. The contingency plan did not provide the system user with a work around or a list of procedures to follow in the event of a Y2K contingency. Instead, the contingency plan directed the system user to implement the continuity-of-operations plan and to report the system failure to the NAVSSES in-service engineer. Also, the contingency plan did not identify specific procedures that the system user was to follow to recognize system degradation, to detect corrupt data within the system, and to preserve and protect data as a result of a Y2K system failure.

Planning Elements. Although the contingency plan identified risks, system impacts, and alternative strategies, it did not describe the mission impacts of those risks.

Overview Elements. The plan system description adequately identified and described the system components and software requirements. The plan validation and testing section adequately addressed contingency plan testing and the organization responsible for testing the contingency plan.

LSD-41 Class Ship Machinery Control System. The Machinery Control System for the LSD-41 Class Ship controls and monitors the propulsion plants and auxiliary equipment.

Preparation Elements. The contingency plan did not provide the system user with a work around or a list of procedures to follow in the event of a contingency. Instead, the contingency plan directed the system user to implement the continuity-of-operations plan and to report the system failure to the NAVSSES in-service engineer. Also, the contingency plan did not identify specific procedures that the system user was to follow to recognize system degradation, to detect corrupt data within the system, and to preserve and protect data as a result of a Y2K-related system failure.

Planning Elements. Although the contingency plan identified risks, the system impacts, and the alternative strategies, it did not describe the mission impacts of those risks.

Overview Elements. The contingency plan system description adequately identified and described the system components and software requirements. The plan validation and testing section states that if the contingency plans were not tested during Navywide end-to-end testing, then NAVSSES in-service engineers would be tasked to test the contingency plan. However, the plan did not identify the organization responsible for tasking the engineers to test the contingency plan.

U.S.S. *Rushmore* (LSD-47) Machinery Control System. The Machinery Control System for the U.S.S. *Rushmore* (LSD-47) is an automated electrical control system that monitors and operates the propulsion and electrical plants and supports auxiliary machinery.

Preparation Elements. The contingency plan did not address preparation elements for the failure of the programmable logic controller, the operator interface application, or the shipboard network. In the event of a Microsoft NT operating system date failure, the contingency plan did not provide the system user with a work around or a list of procedures to follow. Instead, the contingency plan directed the system user to report the system failure to the NAVSSES in-service engineer. Also, the contingency plan did not identify specific procedures that the system user was to follow to recognize system degradation, to detect corrupt data within the system, and to preserve and protect data as a result of a Y2K system failure.

Planning Elements. The contingency plan identified risk and the probability of occurrence; however, the risk of a shipboard network failure occurring was not quantified. Also, the system and mission impacts and alternative strategies for the identified risks were not addressed.

Overview Elements. The contingency plan system description adequately identified and described the system components and software requirements. The contingency plan adequately addressed contingency plan testing.

MCM-1 Machinery Control System. MCM-1 Class Ships use the Machinery Control System to monitor and operate the ship propulsion and firemain systems, the ship power generation and distribution systems, and the ship auxiliary equipment.

Preparation Elements. The contingency plan recommended a work around for two of the six identified risks and directed the system user to implement the continuity-of-operations plan and to report the Y2K problem to the in-service engineer. The contingency plan did not address shipboard procedures to recognize system degradation, detect corrupt data, and preserve and protect data in the event of a Y2K-related system failure.

Planning Elements. The contingency plan identified risks, described system impacts, and listed alternative strategies for those identified risks, but it did not describe the related mission impacts.

Overview Elements. The contingency plan system description adequately identified and described the system components and software requirements. The contingency plan adequately addressed contingency plan testing.

FFG-7 Class Ship Propulsion Control System. The Propulsion Control System for the FFG-7 Class Ship provides the control and data displays required for starting, controlling, monitoring, and stopping the propulsion system and related equipment.

Preparation Elements. The contingency plan did not provide the system user with a work around or a list of procedures to follow in the event of a contingency. Instead, the contingency plan directed the system user to implement the continuity-of-operations plan and to report the system failure to the NAVSSES in-service engineer. Also, the contingency plan did not identify specific procedures that the system user was to follow to recognize system degradation, to detect corrupt data within the system, and to preserve and protect data in the event of a Y2K system failure.

Planning Elements. The contingency plan identified risks, described system impacts, and listed alternative strategies for those identified risks. However, the contingency plan did not describe the mission impacts of the related risks.

Overview Elements. The contingency plan system description adequately identified and described the system components and software requirements. The plan did not identify the organization responsible for tasking the NAVSSES engineers to perform validation and testing if the contingency plan was not tested during Navywide end-to-end testing.

Contingency Plan Preparation

Contingency Plan Tasking. On November 17, 1998, the Integrated Information Systems Engineering Group Y2K point of contact tasked NAVSSES in-service engineers to prepare contingency plans for mission-critical HM&E systems. The in-service engineers were to prepare the contingency plans using the criteria in the Navy Contingency and Continuity-of-Operations Planning Guide.

Contingency Plan Approval. On December 1, 1998, the Director, Integrated Information Systems Engineering Group, approved the NAVSSES-prepared contingency plans; submitted the plans to the Naval Sea Systems Command Y2K Project Office; and stated that in the event of an "operational failure," the contingency plans provide the detailed course of action for mission sustainability.

Contingency Plan Quality Assurance Review. The Integrated Information Systems Engineering Group did not have an effective quality assurance process for reviewing contingency plans. The Integrated Information Systems Engineering Group did have a quality assurance review process in place, but they expected the NAVSSES in-service engineers to provide contingency plans that did not require in-depth review and analysis. Consequently, the Integrated Information Systems Engineering Group reviewed the contingency plans only to ensure that the plans included the preparation, planning, oversight, execution, and recovery elements, instead of making a substantive review of the content of those elements.

Summary

The surface ship hull, mechanical, and electrical system contingency plans did not always address the Navy Y2K contingency plan elements of preparation, planning, and overview. Although the contingency plans directed system users to implement the continuity-of-operations plan if a Y2K problem occurred, the contingency plans did not clearly show the link between implementing the contingency plan with the procedures that are outlined in the engineering operational sequencing system. Also, the contingency plans did not provide procedures to recognize system degradation, to detect corrupt system data, and to preserve and protect data.

Recommendations and Management Comments

We recommend that the Director, Integrated Information Systems Engineering Group, Naval Sea Systems Command:

1. Establish a more effective quality assurance review process to ensure that contingency plans meet the Navy Y2K contingency and continuity-of-operations planning guide criteria.

Management Comments. The Navy concurred and stated that the Integrated Information Systems Engineering Group has begun taking steps to improve its quality assurance review process. The Navy has started a disciplined implementation of the three-tiered review process and engaged an independent contractor to assist in contingency plan reviews.

2. Revise the hull, mechanical, and electrical contingency plans that do not adequately address the overview, planning, and preparation elements specified in the Navy Y2K contingency and continuity-of-operations planning guide.

Management Comments. The Navy concurred and stated that the Integrated Information Systems Engineering Group revised all contingency plans to reflect issues raised by the audit team, and on March 16, 1999, submitted the revised contingency plans to the Y2K project office for fleet review.

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 capability challenge. For a list of audit projects addressing this issue, see the Y2K webpage on IGnet at http://www.ignet.gov.

Scope

Work Performed. We reviewed Y2K certification procedures for surface ship HM&E systems to determine whether those procedures met the Navy Y2K requirements. We reviewed contingency plans for 14 HM&E systems to determine whether the contingency plans addressed the overview, planning, and preparation elements. We also reviewed initialization procedures for six HM&E systems to determine whether those procedures described the steps required for system users to conduct Y2K tests, document the results of those tests, and reset the system to the correct date and time.

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 an 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 and 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 reviewed Y2K

documents dated from August 1998 through February 1999 and evaluated the Integrated Information Systems Engineering Group efforts at certifying systems as Y2K compliant and preparing contingency plans and initialization procedures.

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from October 1998 through February 1999, in accordance with 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 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.

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

Year 2000 Testing and Certification Procedures

The Integrated Information Systems Engineering Group managed the Y2K certification of HM&E systems. We reviewed the Y2K testing and certification procedures and found that HM&E systems were tested for Y2K rollover, leap year, and the processing of dates in the 1900s and 2000s.

Initialization Procedures

The Integrated Information Systems Group directed NAVSSES in-service engineers to prepare initialization procedures for all vulnerable HM&E systems. We reviewed these procedures and found that they provided system users with steps to roll over the system date, record data observations, and restore the system to the correct date.

Embedded Microprocessors

Embedded microprocessors are silicon integrated circuits that generally contain permanently coded instructions. The chips generally take the form of microprocessors, timers, sequencers, or controllers built into systems to monitor, regulate, or control the operation of that system.

The Integrated Information Systems Group collaborated with the Aircraft Carrier Program Executive Office and tasked the NAVSSES in-service engineers to analyze over 35,000 HM&E parts. NAVSSES found only two parts with embedded chips, and both were Y2K compliant. Also, the Integrated Information Systems Group is working with NAVSSES in-service engineers to prioritize and review HM&E systems for embedded chips.

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 Assistant Secretary of Defense (Command, Control, Communications, and Intelligence, Surveillance, Reconnaissance, and Space Systems)
  Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
    Principal Director for Year 2000
Assistant to the Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the 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)
Auditor General, Department of the Navy
Chief Information Officer, Department of the Navy
  Navy Year 2000 Project Office
Commander, Naval Sea Systems Command
  Deputy Commander for Engineering
    Director, Integrated Information Systems Engineering Group
Inspector General, Department of the Navy
Inspector General, Marine Corps

Department of the Air Force

Auditor General, Air Force Audit Agency
Inspector 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 Office
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

14 May 99

MEMORANDUM FOR THE DEPARTMENT OF DEFENSE ASSISTANT INSPECTOR GENERAL FOR AUDITING

Subj: AUDIT REPORT ON YEAR 2000 CONTINGENCY PLANS FOR SURFACE SHIP HULL, MECHNANICAL, AND ELECTRICAL SYSTEMS (PROJECT NO. 8AD-0053.00)

Ref: (a) DODIG memo of 7 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 contingency plans for Surface Ship hull, mechanical, and electrical systems (project no. 8AD-0053.00).

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 findings and recommendations in the draft report. The Commander, Naval Sea Systems Command takes 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 YEAR 2000 CONTINGENCY PLANS FOR SURFACE SHIP HULL, MECHNANICAL, AND ELECTRICAL SYSTEMS (PROJECT NO. 8AD-0053.00)

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
Naval Inspector General
Inspector General Marine Corps
Naval Audit Service
USMC CIO
USN Y2K Project Office
NAVINSGEN(02)
ASSTSECNAV FM&C (FMO-31)
COMMNAVSEASYSCOM

Final Report Reference

NAVY RESPONSE TO
DODIG DRAFT AUDIT REPORT ON
YEAR 2000 CONTINGENCY PLANS FOR SURFACE SHIP
HULL, MECHANICAL, AND ELECTRICAL SYSTEMS
PROJECT NO. 8AD-0053 OF 7 APRIL 1999

Overall Comment:

Page 12 paragraph 3, Contingency Plan Preparation Page 11

Audit comment: The Integrated Information Systems Engineering Group did have a quality assurance review process in place, but they expected the NAVSSES in-service engineers to provide contingency plans that did not require in-depth review and analysis.

Navy Response: Concur - A quality assurance review process for all deliverables (including contingency plans) submitted by the in-service engineering agents at Carderock Division, Naval Surface Warfare Center - Philadelphia Detachment (CD NSWC) does exist. Contingency plans (CPs) are developed by subject matter experts at CD NSWC, reviewed and approved by their management and then delivered to the CD NSWC Y2K Team Leader for further review and approval. The CPs are then delivered to the CD NSWC Technical Director for final review and approval prior to delivery to the Naval Sea Systems Command (NAVSEA) Code 03J Y2K Team Leader. The NAVSEA engineering groups (including Code 03J) expect that this process will result in products that are of adequate quality and normally should not require further in-depth review at the headquarter level.

Page 12 paragraph 4, Summary Page 11

Audit Comment: The contingency plans did not clearly show the link between implementing the contingency plan with the procedures that are outlined in the engineering operational sequencing system (EOSS.)

Navy Response: Concur - NAVSEA provided additional information to DOD IG representatives to demonstrate the relationship between CPs and EOSS. On 25 March 1999 NAVSEA Code 03J provided to DOD IG representatives amplifying information describing what EOSS is and what it does. That documentation reiterated the requirement for ship personnel familiarity with, and the process for implementing the procedures of EOSS. Additionally, on April 1, 1999, NAVSEA

Enclosure (1)

Final Report Reference

Codes 05 and 03J, Team Submarine, and the Program Manager (PM) for the Cooperative Engagement Capability (CEC) system made presentations to additional DOD IG representatives to demonstrate the relationship between CPs and EOSS/Combat Systems Operating Sequencing System (CSOSS) by:

1. Describing what EOSS/CSOSS are and what they do,
2. Emphasizing that ship personnel are trained to automatically employ casualty control procedures such as EOSS/CSOSS at any time that a system does not perform as intended (for any reason, including potential disruptions resulting from Y2K type problems).
3. Emphasizing that ship personnel clearly understand the link between CPs and EOSS/CSOSS.
4. Emphasizing that EOSS/CSOSS have built-in procedures for work-arounds during casualty situations.
5. Showing how the CPs and the EOSS/CSSOS compliment each other, rather than being duplicative or disconnected.

At that meeting, the DOD IG representatives commented that they had a better appreciation for the approach that NAVSEA has taken regarding references to existing system documentation such as EOSS in CPs. They commented that step-by-step procedures should be included in CPs for systems that are not associated with casualty control procedures such as EOSS/CSOSS.

Page 11

Page 12 paragraph 4, Summary

Audit comment: The contingency plans did not provide procedures to recognize system degradation, to detect corrupt system data and to preserve and protect data.

Navy Response: Concur - On April 1, 1999 NAVSEA Codes 05, 03J, Team Submarine, and the PM for CEC made presentations to DOD IG representatives stating that ship personnel are trained to recognize and respond automatically to any system mal-operation, degradation or data corruption regardless of the cause(s). NAVSEA representatives stated that a distinction of the failure mode would be made when a mal-operation is appropriately attributable to a Y2K related issue. Since shipboard personnel are operators rather than technical experts for HM&E vulnerable systems, personnel should defer to technical experts ashore such as the Fleet Technical Support Centers or the In-Service Engineering Agent to preserve and protect the data of a system that malfunctions.

Page 13, Comments on Recommendations:

We recommend that the Director, Integrated Information Systems Engineering Group, Naval Sea Systems Command:

1. Establish a more effective quality assurance review process to ensure that contingency plans meet the Navy Y2K contingency and continuity of operations planning guide criteria.

Navy response to Recommendation 1: Concur - Due to the criticality of Y2K preparation and issues raised during the February 4, 1999 meeting between DOD IG and NAVSEA Code 03J representatives, NAVSEA Code 03J took positive, proactive steps to strengthen the existing review process. The steps included a more rigorous and disciplined implementation of the three tiered review process. Additionally, Code 03J is applying more in-depth reviews of products delivered by CD NSWC. Code 03J has engaged independent contractor support to assist with the review process.

2. Revise the hull, mechanical, and electrical contingency plans that do not adequately address the overview, planning, and preparation elements specified in the Navy Y2K contingency and continuity-of-operations planning guide.

Navy response to Recommendation 2: Concur - NAVSEA Code 03J revised all of the HM&E contingency plans to reflect issues raised by the DOD IG. On March 16, 1999, NAVSEA 03J submitted revised CPs to the Y2K project office for fleet review.

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
Marvin E. Tuxhorn