Audit Report

YEAR 2000 COMPLIANCE OF THE
TRIDENT SUBMARINE COMMAND AND CONTROL SYSTEM

Report Number 99-167 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

CCS	Command and Control System
Y2K	Year 2000

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

May 24, 1999

MEMORANDUM FOR COMMANDER IN CHIEF, U.S. PACIFIC COMMAND
ASSISTANT SECRETARY OF THE NAVY (FINANCIAL MANAGEMENT AND COMPTROLLER)

SUBJECT: Audit Report on Year 2000 Compliance of the Trident Submarine Command and Control System (Report No. 99-167)

We are providing this report for your information and use. This report is one in a series being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor efforts to address the year 2000 computing challenge. Because this report contains no findings or recommendations, no written comments were required, and none were received.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Joseph Doyle at (703) 604-9348 (DSN 664-9348) or Mr. John Yonaitis at (703) 604-9340 (DSN 664-9340). See Appendix C for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-167 **May 24, 1999**
(Project No. 9CC-0086.05)

Year 2000 Compliance of the *Trident* Submarine Command and Control System

Executive Summary

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

Objectives. The overall audit objective was to assess the status of Military Department and Defense agency mission critical systems, identified by the U.S. Pacific Command and U.S. Forces Korea, as being of particular importance to them in attaining compliance with year 2000 conversion requirements. Specifically, we reviewed the progress of each system toward year 2000 compliance, testing and integration of modifications, and contingency plans. For this report, we reviewed the *Trident* Submarine Command and Control System, revisions 5.5 and 6.3.

Results. The *Trident* Submarine Command and Control System, revisions 5.5 and 6.3 were certified year 2000 compliant in September 1998. The program manager followed the Navy certification process and documented the system verification, testing, interfaces, implementation, and contingency plan. The implementation of the command and control system, revisions 5.5 and 6.3 has been completed for 13 of the 18 *Trident* submarines and is on schedule for the remaining 5 *Trident* submarines.

Management Comments. We provided a draft of this report on April 27, 1999. Because this report contains no findings or recommendations, written comments were not required, and none were received. Therefore, we are publishing this report in final form.

Table of Contents

Executive Summary i

Introduction

Background 1
Objectives 1

Discussion

Year 2000 Compliance of the *Trident* Submarine Command and Control System 2

Appendixes

A. Audit Process
Scope 4
Methodology 5
Summary of Prior Coverage 5
B. Implementation Schedule 6
C. Report Distribution 7

Background

The Executive Order, "Year 2000 Conversion," February 4, 1998, mandates that Federal agencies do what is necessary to ensure that no critical Federal program experiences disruption because of the year 2000 (Y2K) computing problem. The Executive Order also requires that the head of each agency ensure that efforts to address Y2K issues receive the highest priority.

The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) is the principal staff assistant responsible for the DoD Y2K management plan. The DoD Y2K Management Plan, version 2, December 1998, provides guidance for testing and certifying systems and preparing contingency plans for those systems, and stipulates the criteria that DoD Components must use to meet reporting requirements.

The Navy Year 2000 Action Plan, September 1998, provides the guidance for planning and implementing all information technology, software and systems in the Navy that face a Y2K problem. The Navy must ensure Y2K readiness of the *Trident* Submarine Command and Control System (CCS).

***Trident* Submarine CCS.** The *Trident* Submarine CCS provides the means for integrating the various subsystems supporting the management of a *Trident* submarine. The subsystems include the following elements: antenna, data processing, defensive weapons, electronics monitoring, exterior and interior communications, periscope, radar, ship command and control, sonar, and tactical navigation systems. The *Trident* Submarine CCS was implemented in revisions 5.5 and 6.3 configurations.

CCS Revisions. Revision 5.5 of CCS is to be implemented on 13 Ohio Class *Trident* submarines, and revision 6.3 of CCS is to be implemented on 5 Ohio Class *Trident* submarines. The implementations are scheduled to be completed by August 1999. See Appendix B for a list of implementations.

Objectives

The overall objective was to assess the status of Military Department and Defense agency mission critical systems, identified by the U.S. Pacific Command and U.S. Forces Korea as being of particular importance to them, in attaining compliance with Y2K conversion requirements. Specifically, we reviewed the progress of each system towards Y2K compliance, testing and integration of modifications, and contingency plans. For this report, we reviewed the *Trident* Submarine CCS, revisions 5.5 and 6.3. See Appendix A for a discussion of the scope and methodology, and a summary of prior coverage.

Year 2000 Compliance of the *Trident* Submarine Command and Control System

The *Trident* Submarine CCS was appropriately certified as Y2K compliant in September 1998. The CCS program manager followed the Navy certification process and properly documented the verification, testing, interfaces, and contingency documentation of the CCS. As a result, the Navy has minimized the risk of year 2000 failure of the CCS. The implementation of the CCS was on schedule.

Y2K Compliance of the CCS

The Strategic and Attack Submarine program office, a part of the Naval Sea Systems Command, is responsible for the CCS with oversight from Headquarters, Department of the Navy. The Naval Undersea Warfare Center, Newport Division, Newport, Rhode Island, conducted the Y2K tests of the CCS, revisions 5.5 and 6.3 and interfaces in March and May 1998, and certified them as year 2000 compliant in September 1998.

CCS Revision 5.5 and 6.3 Tests. The Naval Undersea Warfare Center, Newport Division, performed system testing from March 2 to 16 and from May 6 to June 8, 1998. The revisions were evaluated and four primary tests were performed including: date processing for the 20th and 21st centuries; date processing between the 20th and 21st centuries; and data transfers across interfaces. The revisions passed all of the tests and were certified as Y2K compliant on September 16, 1998. However, a revised certification was signed on April 8, 1999 updating the original certification to include the DoD certification level.

CCS Interfaces. The CCS interfaces with the Integrated Radio Room and Strategic Weapon Systems. The Naval Undersea Warfare Center, Newport Division, successfully conducted Y2K interface testing in March and May 1998 and determined the interfaces to be Y2K compliant with the CCS.

Implementation Plan

Revision 5.5 of the CCS is to be implemented on 13 Ohio Class *Trident* submarines, and revision 6.3 of the CCS is to be implemented on 5 Ohio Class *Trident* submarines. As of March 1999, implementation was still required on 4 of the 13 submarines receiving revision 5.5, and on 1 of the 5 submarines receiving revision 6.3. Implementation is dependent on the submarine schedule. The implementations are scheduled to be completed by August 1999. See Appendix B for an implementation schedule.

Contingency Management Plan

The *Trident* CCS program manager prepared and approved a Y2K contingency plan for *Trident* CCS, revisions 5.5 and 6.3 in December 1998. The purpose of the plan was to ensure the continued effective operation of the *Trident* CCS into and beyond the Y2K. The plan identified specific risks and the likelihood of occurrence. The plan identified alternative strategies for recovering from failure, procedures for implementing the plan, reporting failures, and recovering lost or damaged data.

Conclusion

The *Trident* Submarine CCS program manager complied with DoD and Navy guidance in processing the CCS, revisions 5.5 and 6.3 Y2K certification. The CCS, revisions 5.5 and 6.3 have been determined to be Y2K compliant. The *Trident* Submarine CCS program manager is on schedule to implement the CCS, revisions 5.5 and 6.3 on *Trident* submarines. Therefore, we have no recommendations.

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 web page on the IGnet at http://www.ignet.gov.

Scope

We reviewed and evaluated the *Trident* Submarine CCS, revisions 5.5 and 6.3. We visited the Naval Sea Systems Command program management office responsible for the *Trident* Submarine CCS and met with officials to obtain the year 2000 status of the mission critical system. During our meetings, we obtained data pertaining to the *Trident* Submarine CCS.

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

> **Objective:** Prepare now for an uncertain future. **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key war fighting 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 objectives and goals.

- **Information Technology Management Functional Area.**
  Objective: Become a mission partner. **Goal:** Serve mission information users as customers. **(ITM-1.2)**

- **Information Technology Management Functional Area.**
  Objective: Provide services that satisfy customer information needs.
  Goal: Modernize and integrate DoD information infrastructure.
  (ITM 2.2)

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

Methodology

Audit Type, Dates, and Standard. We performed this program audit in March and April 1999, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did not use computer-processed data to perform this audit.

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

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

Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to the 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. Implementation Schedule

Submarine Name	Submarine Number	Revision Number	Implementation Date
U.S.S. *Alabama*	SSBN-731*	5.5	September 1998
U.S.S. *Alaska*	SSBN-732	5.5	July 1998
U.S.S. *Florida*	SSBN-728	5.5	May 1998
U.S.S. *Georgia*	SSBN-729	5.5	September 1998
U.S.S. *Henry M. Jackson*	SSBN-730	5.5	July 1998
U.S.S. *Kentucky*	SSBN-737	5.5	August 1999**
U.S.S. *Louisiana*	SSBN-743	6.3	February 1999
U.S.S. *Maine*	SSBN-741	6.3	March 1999
U.S.S. *Maryland*	SSBN-738	5.5	October 1998
U.S.S. *Michigan*	SSBN-727	5.5	May 1998
U.S.S. *Nebraska*	SSBN-739	5.5	May 1999**
U.S.S. *Nevada*	SSBN-733	5.5	April 1998
U.S.S. *Ohio*	SSBN-726	6.3	March 1999
U.S.S. *Pennsylvania*	SSBN-735	5.5	May 1999**
U.S.S. *Rhode Island*	SSBN-740	5.5	April 1999**
U.S.S. *Tennessee*	SSBN-734	6.3	March 1999
U.S.S. *West Virginia*	SSBN-736	5.5	December 1998
U.S.S. *Wyoming*	SSBN-742	6.3	April 1999**

* SSBN Ship Submersible Ballistic Nuclear.
** Planned implementation date (dependent on ship availability).

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)
  Under Secretary of Defense for Personnel and Readiness
  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 Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor 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, Navy
Commander, Naval Sea Systems Command

Department of the Air Force

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

Unified Commands

Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Atlantic Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. Special Operations Command

Defense Organizations

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, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
General Accounting Office
  National Security and International Affairs Division,
    Technical Information Center,

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
Senate Committee on Intelligence
House Committee on Appropriations
House Subcommittee on National Security, Committee on Appropriations
House Committee on Armed Services
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
House Permanent Select Committee on Intelligence

Audit Team Members

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

Paul J. Granetto
Joseph P. Doyle
John Yonaitis
John G. LaBelle
Kelly D. Garland