Audit Report

YEAR 2000 COMPLIANCE OF THE STANDARD
ARMY AMMUNITION SYSTEM-MODERNIZATION

Report No. 99-189 June 18, 1999

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or Fax (703) 604-8932 or visit the Inspector General, DoD, Home Page at· www dodig osd mil

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932 Ideas and requests can also be mailed to

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

Defense Hotline

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

Acronyms

SAAS-MOD	Standard Army Ammunition System-Modernization
PEO STAMIS	Program Executive Office for Standard Army Management Information Systems
PM GCSS-A	Project Manager for Global Combat Support System-Army
Y2K	Year 2000

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

June 18, 1999

MEMORANDUM FOR DEPUTY UNDER SECRETARY OF DEFENSE
(LOGISTICS)
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT Audit Report on Year 2000 Compliance of the Standard Army Ammunition System-Modernization (Report No 99-189)

We are providing this report for information and use This report 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 efforts to address the year 2000 computing challenge Because this report contains no 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. Tilghman A. Schraden at (703) 604-9186 (DSN 664-9186) (tschraden@dodig.osd.mil) or Mr. Thomas D. Kelly at (215) 737-3886 (DSN 444-3886) (tkelly@dodig.osd.mil). See Appendix B for the report distribution The audit team members are listed inside the back cover

Robert J Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-189 **June 18, 1999**
(Project No 9LH-5039)

Year 2000 Compliance of the Standard Army Ammunition System-Modernization

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 efforts to address the year 2000 computing challenge. For a list of audit projects addressing the issue, see the year 2000 webpage on the IGnet at http //www ignet gov/.

Within the Army, the Program Executive Officer for Standard Army Management Information Systems is responsible for the implementation, execution, testing, and operational performance of year 2000 efforts associated with the Standard Army Ammunition System-Modernization (SAAS-MOD) SAAS-MOD is a mission-critical system that was developed and fielded by the Project Manager for Global Combat Support Systems-Army (formerly the Project Manager, Integrated Logistics Systems) SAAS-MOD automates ammunition management functions in the Army Corps and Theater Materiel Management Centers to include the issue, receipt, shipping and storage operations at ammunition supply points. SAAS-MOD consists of hardware (usually a personal or lap top computer) and a software suite of server, workstation (operating and application programs), and communication As of March 31, 1999, 178 systems had been issued 90 to active Army units, 23 to Army Reserve units, and 65 to National Guard units. The fielding of 226 systems is to be completed by July 2, 1999.

Objectives. The overall audit objective was to evaluate whether DoD was adequately planning for and managing year 2000 risks for selected logistics systems to avoid disruption of the DoD mission. Specifically, we reviewed the year 2000 risk assessments, testing, and contingency planning for selected logistics systems that support the DoD mission. We selected mission-critical logistics systems that were of particular importance to the Director, Logistics Systems Modernization, Office of the Deputy Under Secretary of Defense (Logistics). For this report, we reviewed the SAAS-MOD.

Results. The Program Executive Office for Standard Army Management Information Systems Year 2000 Project Office and the Project Manager for Global Combat Support System-Army Project Office adequately planned for and managed year 2000 risks for the SAAS-MOD Although the December 31, 1998, milestone that the DoD Year 2000 Management Plan established for implementation was exceeded, the Program Executive Office for Standard Army Management Information Systems and the Project Manager for

Global Combat Support Systems-Army took effective action to ensure that SAAS-MOD was certified in time to participate in logistics end-to-end testing that was scheduled to begin in May 1999 The Program Executive Office for Standard Army Management Information Systems and the Project Manager for Global Combat Support Systems-Army estimated that a year 2000 compliant SAAS–MOD would be implemented at all active Army units by June 1999. See Finding section of report for details on the audit results

Management Comments. We provided a draft of this report on May 28, 1999 Because this report contains no 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 2

Finding

Year 2000 Compliance of the Standard Army Ammunition System-Modernization 4

Appendixes

A. Audit Process
Scope 9
Methodology 10
Summary of Prior Coverage 10
B Report Distribution 11

Background

Executive Order. 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 requires that the head of each agency ensure that efforts to address Y2K issues receive the highest priority in the agency.

DoD Y2K Management Plan. The "DoD Year 2000 (Y2K) Management Plan," (DoD 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 DoD Y2K Management Plan makes the principal staff assistants of the Office of the Secretary of Defense responsible for verifying that all functions under his or her purview will continue unaffected by Y2K issues The principal staff assistant for logistics is the Under Secretary of Defense for Acquisition and Technology The DoD Y2K Management Plan requires each principal staff assistant to

- provide plans for functional end-to-end testing,
- certify that test plans include assessments of functional risk,
- ensure that test plans include listings of all mission-critical systems included in the test, and
- coordinate each test plan with the Military Departments and all other pertinent principal staff assistants.

The target implementation date for all mission-critical systems was December 31, 1998. Some logistics systems were not compliant, so the Director for Logistics Systems Modernization, Office of the Deputy Under Secretary of Defense (Logistics), requested the Inspector General, DoD, to examine what was being done to ensure that those systems were made compliant in time to participate in end-to-end testing, which was scheduled to begin in May 1999

Army Year 2000 Action Plan. The "Army Year 2000 (Y2K) Action Plan," revision II, June 1998, outlines the Army Y2K management strategy, provides guidance, and defines roles, responsibilities, and reporting requirements The plan applies to all systems supported by information technology, their technical environment, and their communications devices

Program Executive Office for Standard Army Management Information Systems. The Program Executive Office for Standard Army Management Information Systems (PEO STAMIS) was established in 1987 as part of the implementation of the Goldwater-Nichols Act. The mission of the PEO STAMIS is to plan, design, develop, acquire, install, and maintain complex management information systems as directed by the Army Acquisition Executive In July 1997, the PEO STAMIS established a Y2K project office to monitor and support the planning, resourcing, testing, certifying, and implementing of Y2K solutions for PEO STAMIS systems The PEO STAMIS established the Y2K project office to ensure that no critical system failure occurs because of Y2K related problems The PEO STAMIS is responsible for about 47 Army management information systems, one of which is the Standard Army Ammunition System-Modernization (SAAS-MOD)

Standard Army Ammunition System-Modernization. SAAS–MOD is a mission-critical system that was developed and fielded by the Project Manager for Global Combat Support Systems-Army (PM GCSS-A) (formerly the Project Manager, Integrated Logistics Systems). SAAS-MOD automates ammunition management functions in the Army corps and theater materiel management centers to include the issue, receipt, shipping, and storage operations at ammunition supply points SAAS-MOD consists of hardware (usually a personal or lap top computer) and a software suite of server, workstation (operating and application programs), and communication As of March 31, 1999, 178 systems had been issued. 90 to active Army units, 23 to Army Reserve units, and 65 to National Guard units. The fielding of 226 systems is to be completed by July 2, 1999

SAAS-MOD receives, processes, and sends data to several systems, using magnetic media or communications networks to accomplish all interfaces All data received by communications are normally batch processed after the communications portion of the interface is complete SAAS-MOD interfaces with the Commodity Command Standard System, the Defense Automated Address System, the Logistics Support Activity, the Standard Property Book System-Redesign, the Training Ammunition Management Information System, the Unit Level Logistics System, and the Worldwide Ammunition Reporting System

Objectives

The overall audit objective was to evaluate whether DoD was adequately planning for and managing Y2K risks for selected logistics systems to avoid disruption to the DoD mission Specifically, we reviewed the Y2K risk assessments, testing, and contingency planning for selected logistics systems that support the DoD mission We selected mission-critical logistics systems that

were of particular importance to the Director, Logistics Systems Modernization, Office of the Deputy Under Secretary of Defense (Logistics) For this report, we reviewed the SAAS–MOD See Appendix A for a discussion of the scope and methodology and for a summary of prior coverage

Year 2000 Compliance of the Standard Army Ammunition System-Modernization

The PEO STAMIS and the PM GCSS-A adequately planned for and managed Y2K risks for the SAAS - MOD PEO STAMIS and PM GCSS-A followed the DoD Management Plan in assessing risks, renovating fixes, validating performance, implementing improvements, and planning for end-to-end testing Although the December 31, 1998, milestone that the DoD Management Plan established for implementation was exceeded, PEO STAMIS and the PM GCSS-A took effective action to ensure that SAAS-MOD was certified in time to participate in logistics end-to-end testing that was scheduled to begin in May 1999 PEO STAMIS and PM GCSS-A estimated that a Y2K compliant SAAS-MOD would be implemented at all Active Army units by June 1999

Criteria for Managing Y2K Conversion Efforts

DoD Management Plan. The DoD Management Plan includes a description of the five–phase Y2K Management Process that the DoD Components were to follow The first phase was to promote awareness of the Y2K problem across the Component and all levels of leadership This phase was to be completed in December 1996 The other four phases, oriented more toward specific systems, were to be completed by December 31, 1998, as described below

- Assessment Phase DoD Components were to inventory all systems, identify mission critical systems, assess each system for Y2K risks and issues, develop a strategy for addressing each risk, prioritize all systems for correcting risks, and develop contingency plans Target completion date was June 30, 1997

- Renovation Phase DoD Components were to replace, repair, or terminate systems to ensure Y2K compliance Target completion date for mission-critical systems was June 30, 1998

- Validation Phase DoD Components were to test and certify systems for Y2K compliance. Target completion date for mission-critical items was September 30, 1998

- Implementation Phase DoD Components were to fully deploy renovated and replacement systems Target completion date for mission-critical systems was December 31, 1998

In addition to the five-phase management process, Appendix I of the DoD Management Plan requires DoD Components to achieve a level of confidence above individual system testing by conducting end-to-end testing End-to-end testing, which tests a system's ability to process information to and from interface systems, is to be conducted as part of either joint Service evaluations, Service-sponsored integration tests, or functional area tests

Y2K Implementing Guidance. PEO STAMIS and PM GCSS-A issued supplemental guidance to the DoD Management Plan and the Army Y2K Action Plan. PEO STAMIS published "Program Executive Officer's Year 2000 Technical Assessment Process Handbook," June 1997, and "PEO STAMIS Year 2000 Program Management Plan," release 2, August 1998 In May 1998, PM GCSS-A published "PM ILOGS [Project Manager Integrated Logistics Systems] Y2K Compliance Plan "

Assessing Risk

Y2K Risk. PEO STAMIS and PM GCSS-A followed the DoD Management Plan in making a risk assessment At the initiation of the PEO STAMIS, the Computer Science Corporation conducted a Y2K risk assessment of the SAAS–MOD from April 22 through May 30, 1997 – about a month before the required date established by the DoD Management Plan. The assessment was made to identify risks and concerns with the SAAS-MOD hardware and software In addition to identifying risks and concerns, two of the most important aspects of completing a risk assessment – obtaining interface agreements and preparing contingency plans – were properly accomplished. The Computer Science Corporation's assessment was that SAAS-MOD was Y2K-compliant except for minor hardware problems. The Computer Science Corporation analyzed 32 hardware components Of the 32 components, 24 were not date-dependent, 4 were fully compliant, and 4 were partially compliant Four components were partially compliant because they could house noncompliant basic input-output systems Basic input-output systems keep track of the date and time within microcomputers, and those produced before July 1995 could (depending on the manufacturer) fail at the turn of the century because they will not advance the century date For SAAS–MOD, those basic input-output systems were isolated to early models issued to units in Germany.

Operational Environment Risk. In its operational environment, the SAAS-MOD critical performance thread (requisitioning processing) is not essential to users from a time standpoint Requisitioning processing time is relatively unimportant to users because they only requisition ammunition for replenishment of reserve amounts, and wholesale organizations only issue ammunition after they have consolidated enough requisitions to move the ammunition in bulk, usually by ship Accordingly, the receipt of ammunition by users would be unaffected by

using alternate methods for requisitioning ammunition For example, users could mail or E-mail requisitions to wholesale organizations for processing the requisitions, and users would receive the ammunition that was requisitioned within the same time frame as if the requisition was processed by SAAS-MOD

Obtaining Interface Agreements. PEO STAMIS and PM GCSS-A followed the DoD Management Plan in obtaining interface agreements The DoD Management Plan requires system owners to identify system data exchange interfaces and to prepare agreements regarding formats and protocols The agreements are to document the strategy between system owners for sending and receiving information PEO STAMIS and PM GCSS-A had obtained all necessary interface agreements with owners of other systems by March 1998. The agreements essentially provided that the sending system would continue to provide date information in the same format and that the receiving system would make any changes necessary to accommodate the format of the sending system The agreements covered all essential elements required by the DoD Management Plan

Preparing Contingency Plans. PEO STAMIS and PM GCSS-A followed the DoD Management Plan in preparing contingency plans The DoD Management Plan requires two types of contingency plans a system contingency plan that focuses on restoring a system and an operational contingency plan that focuses on how to complete a mission or function without the support of the system PM GCSS-A published the SAAS-MOD contingency plan in April 1998, about 8 months before the plan was required by the DoD Management Plan The U S Army Combined Arms Support Command published the operational contingency plan in January 1999, about 3 months before the plan was required by the DoD Management Plan. The system and operational plans addressed the essential requirements of the DoD Management Plan, such as delineating response and protection procedures, backing up records, switching to alternate locations, and performing operations manually The operational contingency plan will be exercised in September 1999 as part of an overall operational evaluation in the Pacific Theater

Renovating System

PEO STAMIS and PM GCSS-A followed the DoD Management Plan in renovating SAAS-MOD, except they did not meet the established time frame To address the partially compliant issue raised by the SAAS-MOD risk assessment, PEO STAMIS and PM GCSS-A engaged the Signal Corporation and the U.S Army Information Systems Software Development Center, Fort Lee. The solution selected by the PEO STAMIS and the PM GCSS-A was to have a technician go to Germany and upgrade the input-output systems so that SAAS-MOD would automatically reflect the correct date after the end of 1999 (the date could also be changed manually after the end of 1999) However, in testing the solution, a problem surfaced with 710 lines of coding that were in the SAAS-MOD application program. Unless corrected, the 710 lines of coding could

affect the record sorting process and result in incorrect date headings on management reports To solve the problem, the Signal Corporation, the Software Development Center, the TRW Corporation, and selected users successfully developed and tested compact discs that would automatically change the coding The successful testing was completed in November 1998, about 5 months after the renovation phase was to be completed.

Validating Performance

PEO STAMIS and PM GCSS-A followed the DoD Management Plan in validating the compliance of SAAS-MOD, except they did not meet the established time frame To test the compliance of SAAS–MOD independently, PEO STAMIS and PM GCSS-A engaged TRW Corporation The independent verification test consisted essentially of SAAS–MOD demonstrating the capability to carry out all its functions while passing through five timing sequences PEO STAMIS certified SAAS-MOD as Y2K compliant on March 5, 1999 – about 6 months after the validation phase was to be completed Delays in completing the renovation phase and in coming up with a test plan that adequately addressed the requirements of the DoD Management Plan were the leading factors in not completing the validation phase on time. To speed up the Y2K conversion effort and to ensure that SAAS-MOD, as well as other systems, would be available for logistics end-to-end testing scheduled for April 1999, PEO STAMIS established an Army action team in November 1998 The team was headed by the Deputy PM GCSS-A and its members were from the Office of the Deputy Chief of Staff for Logistics, PEO STAMIS, and the U S Army Information Systems Software Development Center- Fort Lee. Representatives from TRW Corporation also provided independent verification and validation support to the team The team members were assigned on a full-time basis and as of March 31, 1999, all PM GCSS-A logistics systems were certified Y2K compliant

Implementing Improvements

PEO STAMIS and PM GCSS-A followed the DoD Management Plan in transitioning SAAS-MOD to a fully compliant Y2K environment As of March 31, 1999, PEO STAMIS and PM GCSS-A had issued 154 compact discs with updated coding that was Y2K compliant to all users of SAAS–MOD that had not received the new models PEO-STAMIS and PM GCSS-A had followed up with the units to ensure implementation and expected that effort to be completed by June 1999

Planning for End-to-End Testing

PEO STAMIS and PM GCSS-A followed the DoD Management Plan in preparing SAAS-MOD for end–to-end testing SAAS–MOD was selected by the Army functional proponent for logistics to participate in two levels of end-to-end testing, within the Army and outside the Army Because SAAS-MOD operates solely within the Army, it will undergo the same test regardless of the level. The critical performance thread for SAAS-MOD was identified as processing requisitions for ammunition in accordance with Military Standard Requisitioning and Issue Procedures At both levels, it will process requisitions to and receive shipment status from wholesale organizations under various timing sequences In March 1999, we observed that SAAS-MOD had already been configured and was ready for end-to-end testing The tests were planned for May 6 through May 20 within the Army and May 25 through July 16 outside the Army

Conclusion

SAAS-MOD should meet any Y2K challenges It is generally not date dependent, and when the conversion efforts of PEO STAMIS and PM-GCSS-A are considered, its system environment appears unsusceptible to Y2K computer glitches Moreover, its operational environment appears even less susceptible to Y2K computer glitches because users have contingency plans and the SAAS-MOD critical performance thread (requisitioning processing) is not essential to users from a time standpoint

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 this issue, see the Y2K web pages on the IGnet at http //www ignet gov/

Scope

We reviewed and assessed the Y2K compliance status of the SAAS-MOD. The Director, Logistics Systems Modernization, Office of the Deputy Under Secretary of Defense (Logistics) was concerned that SAAS-MOD might not be ready to participate in logistics end-to-end testing We interviewed system and program officials from PEO STAMIS, the PM GCSS-A Project Office, and the Software Development Center We reviewed the DoD Management Plan and documentation on the status of SAAS-MOD, interface agreements, test plans, test reports, contingency plans, and the Army certification process as of April 2, 1999 We used the information from the interviews and documents to assess the Y2K compliance status of SAAS-MOD

DoD-Wide Corporate Level Goals. In response to the Government Performance and Results Act, DoD 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 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 in the Information Technology Management Functional Area

> **Objective:** Become a mission partner. **Goal:** Serve mission information users as customers. **(ITM-1.2)**
>
> **Objective:** Provide services that satisfy customer information needs. **Goal:** Modernize and integrate DoD information infrastructure. **(ITM-2.2)**
>
> **Objective:** Provide services that satisfy customer information needs. **Goal:** Upgrade technology base. **(ITM-2.3)**

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

Methodology

Work Performed. To review the planning for and managing of Y2K risks associated with SAAS-MOD, we ascertained whether the DoD Management Plan was followed in making risk assessments, performing testing, and preparing contingency plans To do so, we interviewed system and program officials and reviewed documentation at the offices of PEO STAMIS, PM GCSS-A, the U S Army Combined Arms Support Command, the Computer Science Corporation, and the U S. Army Information Systems Software Development Center The specific documentation reviewed included risk assessments, interface agreements, test plans, test reports, and contingency plans We did not use computer-processed data to perform this audit

Audit Type, Dates, and Standards. We performed this program audit from February through April 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 reviewed on the Internet at http //www gao gov/ Inspector General, DoD, reports can be reviewed on the Internet at http //www dodig osd mil/

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Deputy Under Secretary of Defense (Logistics)
  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)

Department of the Army

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

Department of the Navy

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

Department of the Air Force

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

Non-Defense Federal Organizations and Individuals

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

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Technology Problem
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Committee on Science

Audit Team Members

The Readiness and Logistics Support Directorate, Office of the Assistant Inspector General, DoD, prepared this report

Shelton R. Young
Raymond D Kidd
Tilghman A Schraden
Thomas D. Kelly
Robert Schonewolf
Paul Hollister
Herman Tolbert
Janice Conte
Glen Wolff