Audit Report

YEAR 2000 STATUS OF THE COMPLIANCE MONITORING AND TRACKING SYSTEM

Report No. D-2000-032 November 5, 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

CMTS	Compliance Monitoring and Tracking System
DTRA	Defense Threat Reduction Agency
Y2K	Year 2000

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

November 5, 1999

MEMORANDUM FOR DIRECTOR, DEFENSE THREAT REDUCTION AGENCY

SUBJECT: Audit Report on Year 2000 Status of the Compliance Monitoring and Tracking System (Report No. D-2000-032)

We are providing this report for information and use. We considered management comments on a draft of this report in preparing the final report.

Comments from the Director, Defense Threat Reduction Agency, were responsive. Management comments conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Ms. Kathryn M. Truex at (703) 604-9045 (DSN 664-9045) (kmtruex@dodig.osd.mil) or Ms. Amy L. Schultz at (703) 604-9074 (DSN 664-9074) (aschultz@dodig.osd.mil). See Appendix C 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. D-2000-032 **November 5, 1999**
(Project No. 9AS-0090.08)

Year 2000 Status of the Compliance Monitoring and Tracking System

Executive Summary

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

The National Defense Authorization Act and the DoD Appropriations Act for FY 1999 require the Inspector General, DoD, to selectively audit information technology and national security systems certified as year 2000 compliant to evaluate the ability of systems to successfully operate during the actual year 2000. The Compliance Monitoring and Tracking System is used to assist in assuring U.S. compliance with a variety of arms control treaties.

Objectives. The overall audit objective was to evaluate the ability of the Compliance Monitoring and Tracking System to operate successfully in the year 2000, including the system's ability to access and transmit information from point of origin to point of termination. Additionally, the audit determined whether an adequate contingency plan exists to ensure continuity of operations and whether the system status reporting has been accurate.

Results. Original audit work questioned the ability of the Compliance Monitoring and Tracking System to operate successfully in the year 2000 because documentation provided by the Defense Threat Reduction Agency did not support the system certification. Additional work performed and additional documentation provided in response to the draft report provided new and adequate assurance that the Compliance Monitoring and Tracking System would operate successfully in the year 2000.

Summary of Recommendations. We recommend that the Director, Defense Threat Reduction Agency, identify all systems that interface with the Compliance Monitoring and Tracking System; obtain interface agreements, including all requirements outlined in the DoD Y2K Management Plan, for each of those interfaces; test all interfaces as part of system level testing; include the Compliance Monitoring and Tracking System in appropriate higher level testing; and recertify the Compliance Monitoring and Tracking System at the appropriate level.

Management Comments. The Defense Threat Reduction Agency comments were responsive to the intent of the recommendations. The Defense Threat Reduction Agency provided additional information necessary for year 2000 certification. Specifically, the Defense Threat Reduction Agency provided a letter from the Program Manager that stated no additional Compliance Monitoring and Tracking System interfaces beyond those identified by the auditors existed, and that interface agreements had been prepared for all interfaces identified. In addition, clarification of interface test documentation was provided, as were functional end-to-end testing documentation and justification for the certification level reported. A discussion of the management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Table of Contents

Executive Summary i

Introduction

Background 1
Objectives 2

Finding

Year 2000 Status of the Compliance Monitoring and Tracking System 3

Appendixes

A. Audit Process
Scope 9
Methodology 10
B. Summary of Prior Coverage 11
C. Report Distribution 13

Management Comments

Defense Threat Reduction Agency 17

The National Defense Authorization Act and the DoD Appropriations Act for FY 1999 require the Inspector General, DoD, to selectively audit information technology and national security systems certified as year 2000 (Y2K) compliant to evaluate the ability of systems to successfully operate during the actual year 2000, including the ability of the systems to access and transmit information from point of origin to point of termination.

Background

DoD Year 2000 Management Strategy. In his role as the DoD Chief Information Officer, the Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), issued the "DoD Year 2000 Management Plan" (DoD Management Plan), version 2.0, in December 1998. The goal of the DoD Management Plan is to ensure the continuance of a mission-capable force able to execute the National Military Strategy before, on, and after January 1, 2000, unaffected by the failure of mission-critical or support systems to properly process date-related information.

Defense Threat Reduction Agency. On October 1, 1998, the Secretary of Defense established the Defense Threat Reduction Agency (DTRA), which is dedicated to reducing the threat of nuclear, chemical, biological, conventional and special weapons to the United States and its allies. Elements of the Office of the Secretary of Defense, the Defense Technology Security Administration, the Defense Special Weapons Agency, and the On-Site Inspection Agency were consolidated as a result of the Secretary's November 1997 Defense Reform Initiative, which directed the creation of DTRA. The DTRA executes technology security activities and cooperative threat reduction programs and monitors arms control treaties and on-site inspections, force protection, and nuclear, biological, and chemical defense and counterproliferation. The DTRA supports the United States' nuclear deterrent and provides technical support on weapons of mass destruction to DoD organizations.

Compliance Monitoring and Tracking System. The Compliance Monitoring and Tracking System (CMTS) is the Government's automated information system designed to assist in ensuring United States compliance with current and pending multilateral and bilateral treaties by allowing storage, secure transmission, and analysis of data under the provisions of the treaties. The CMTS provides for required automated tracking of all Treaty-Accountable Items and Treaty-Limited Items and facilitates the generation, routing, and transmission of exchanged data notifications. Notifications are automatically routed through a review hierarchy to the official U.S. point of contact, the Department of State's Nuclear Risk Reduction Center, and then to the appropriate signatory nations. The DTRA identified CMTS as mission critical.

Objectives

The overall audit objective was to evaluate the ability of CMTS to operate successfully in the year 2000, including the system's ability to access and transmit information from point of origin to point of termination. Additionally, the audit determined whether adequate contingency plans exist to ensure continuity of operations and whether the system status reporting has been accurate. See Appendix A for a discussion of the audit scope and methodology.

Year 2000 Status of the Compliance Monitoring and Tracking System

When initially audited, the ability of CMTS to operate successfully in the year 2000 had not been fully assured. Specifically, DTRA had not:

- identified all system interfaces,
- obtained necessary interface agreements,
- included all interfaces in system level testing,
- included CMTS in the appropriate higher level testing, and
- provided test documentation that supported the certification level reported.

Although DTRA had identified only one interface with CMTS, system documentation and discussions with contractor personnel identified additional interfaces. Also, DTRA personnel maintained that CMTS was not subject to the DoD Management Plan requirement for higher level testing because it was not on a CINC Thinline; however, this was not an exception permitted by the DoD Year 2000 Management Plan. Additional work performed and documentation provided in response to the draft report provided new and adequate assurance that CMTS would operate successfully in the Year 2000.

System Description

System Hardware Components. The CMTS operates through a network of personal computers, SPARCStation servers, and terminal servers. It is a Windows-based computing system consisting of approximately 70 personal computers located throughout the United States and Europe. Treaty information is entered into CMTS through personal computers, transferred via secure data devices or the Secure Internet Protocol Router Network, and stored on the SPARCStation servers. The CMTS processes the information and allows users to monitor treaty requirements and generate, rout, and transmit exchanged data notifications. The exchanged data notifications are used to alert DoD personnel of treaty requirements that require action. Terminal servers connect the personal computers and the SPARCStation servers.

System Software Components. The CMTS operating system is the Solaris V2.6 and it uses Open Ingres for database applications. Mini-hubs are used to create a network that allows the workstations to monitor each other using Qualiz Firstwatch software. Individual workstations use the Windows NT Version 4.0 operating system including Service Packs 3 and 4 and the Microsoft Y2K patches.

DoD Requirements for System Certification.

The following system certification requirements are outlined in the DoD Management Plan.

- Program Managers are required to document system interfaces and obtain interface agreements, or their equivalent, for each system interface.

- DoD Components are required to conduct testing to validate that the systems and all interfaces are Y2K compliant and will perform as intended. Systems must be tested on a compliant domain and in an operationally compliant environment. Mission-critical systems were to be tested and certified appropriately for Y2K compliance by September 30, 1998. Additionally, waivers were to be obtained from the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) for any system that would not be validated in a compliant environment by the January 31, 1999, deadline for nonmission-critical systems.

- Executive software and hardware used by an application must be Y2K compliant for certification. DoD Components may determine a product's Y2K compliance either by vendor compliance information (vendor certifications) or actual hands-on testing.

- The DoD Management Plan requires Principal Staff Assistants to ensure that all mission-critical systems are evaluated at least once in a higher level test, except if the systems are not date dependent or if they operate in a stand-alone environment.

- System and operational contingency plans are required for all mission-critical systems. All plans were to be exercised or validated by June 30, 1999, to ensure that alternate procedures are realistic and executable. Further, contingency plans should be reviewed regularly and modified, if required.

The manner in which DTRA initially addressed each of these requirements is outlined below.

System Interfaces

DTRA recognized only one external interface, the Treaty Inspection Information Management System, for CMTS; however, system documentation and discussions with contractor personnel identified additional interfaces that obtain data to meet the Global Exchange of Military Information and Transparency in Arms treaty requirements. Data from the Strategic Arms Reduction Treaty Tracking and Reporting System and the Strategic Programs Automated

Reporting Treaty Account Notification System are transferred electronically. The DTRA did not recognize these systems as interfaces and therefore did not obtain the necessary interface agreements. DTRA personnel stated that the data for the Global Exchange of Military Information and Transparency in Arms treaties are gathered by an individual who manually enters the information into a database that is loaded into CMTS. However, system documentation states that CMTS servers are able to import data for the Global Exchange of Military Information and Transparency in Arms treaties in electronic form from external databases. Data are imported in database or comma-separated values files on floppy disks into a Microsoft Access 2.0 database resident within the CMTS. Additionally, there could have been other interfaces not yet identified. DTRA needed to evaluate system inputs and outputs to determine whether all interfaces have been identified.

System Certification Testing

System-Level Testing. The CMTS testing did not meet the September 30, 1998, or January 31, 1999, deadlines because the programming was still being performed and the upgrades were not installed. According to DTRA personnel, the programming was a two-year effort that ended with the fielding of the system in April 1999. DTRA officials did not obtain a waiver from the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) because they thought their presentation at a February 1998 Y2K Working Group meeting, which outlined the timelines of the system programming, was sufficient. The Argonne National Laboratory tested CMTS in March 1999. The DTRA personnel stated that all interfaces were tested, as part of the system level testing, however, the test documentation did not support this. A review of CMTS test documentation by Inspector General, DoD, computer engineers indicated that the system itself seemed to have been adequately tested, although the documentation did not support the independent testing required for the level 1a certification.

Component Testing. The DTRA obtained vendor certifications for all CMTS date-dependent hardware and software.

Higher Level Testing

DTRA personnel stated that CMTS was not subject to the DoD Management Plan requirement for higher level testing because it was not on a CINC Thinline. The DoD Management Plan recognizes the difference between mission-critical systems that are on the CINC Thinline and those that are not by requiring two higher level tests for the CINC Thinline systems and one for all other mission-critical systems. Therefore, we concluded that CMTS should participate in at least one higher level test; however, we left the nature of that testing to the discretion of DTRA.

Contingency Planning

CMTS Contingency Planning. DTRA personnel provided the CMTS Continuity of Operations Plan, a system-level plan, dated January 28, 1999. The plan adequately outlines the strategy, policy, procedures, roles and responsibilities, and key personnel necessary to provide reasonable assurance that CMTS will continue to operate after the year 2000. DTRA personnel have not modified the plan since it was originally created in January. The CMTS does not readily fit into any of the DTRA functional area operational plans, but it was included in the DTRA Enterprise Operational Contingency Plan. Although the operational plan does not address CMTS by name, the core functions of CMTS are sufficiently addressed.

Contingency Planning Testing. The DTRA tested its system-level contingency procedures from May 12 though May 17, 1999. The results indicated that notifications could be manually processed within treaty time limits in the event of a Y2K failure of telephone, fax, and computers. The operational contingency plan was tested as part of DTRA tabletop exercises conducted from June 28 though June 30, 1999.

Conclusion

Initial audit results indicated that risks of Y2K failures in the CMTS had not been minimized, because it had not been appropriately certified. Specifically, DTRA had not identified all system interfaces, obtained necessary interface agreements, and included all interfaces in system level testing. Also, the CMTS had not been included in appropriate higher level testing. The DTRA identified only one interface with CMTS; however, system documentation and discussions with contractor personnel identified additional interfaces. Also, DTRA personnel maintained that CMTS was not subject to the DoD Management Plan requirement for higher level testing because it was not on a CINC Thinline; however, this in not an exception permitted by the DoD Management Plan. Additionally, testing documentation did not support the certification level reported by DTRA. Although sound contingency plans exist, it would be preferable to be able to rely on CMTS and avoid system failure. Therefore additional effort should be made to ensure CMTS compliance.

Recommendations, Management Comments and Audit Response

DTRA provided the following comments to the recommendations, but did not explicitly indicate concurrence or nonconcurrence. For the full text of DTRA comments, see the Management Comments section of the report.

We recommend that the Director, Defense Threat Reduction Agency:

1. Identify all systems inputs and outputs to determine a comprehensive list of systems that interface with the Compliance Monitoring and Tracking System;

Management Comments. The DTRA stated that all interfaces with CMTS had been identified. The DTRA provided all supporting documentation for the interface originally identified by DTRA and by the auditors. Additionally, the DTRA CMTS Program Manager signed a statement certifying that no other interfaces existed.

Audit Response. The interface documentation provided with the DTRA response to the draft report adequately addressed concerns regarding identification of interfaces.

2. Obtain interface agreements, including all requirements outlined in the DoD Y2K Management Plan, for each of those interfaces;

Management Comments. The DTRA stated that all interfaces for CMTS had interface agreements. In addition to the interface agreement between CMTS and the Treaty Inspection Information Management System, the DTRA provided interface agreements that it obtained from the Navy, Army, and Air Force on September 21, 1999, and September 23, 1999, for the interfaces identified by the auditors during the audit.

Audit Response. Although the interface agreements included with the DTRA response to the draft audit report did not include all elements suggested by the DoD Y2K Management Plan, DTRA asserted that they were sufficient to ensure coordination among the interfaces after January 1, 2000.

3. Test all interfaces as part of system-level certification testing;

Management Comments. The DTRA stated that all interfaces identified were tested during March 1999; however, the documentation did not specifically identify some of them because they had not been identified as interfaces. The DTRA referenced wording for specific taskings in the documentation requiring the "import" of data, stating that the wording represented the interfaces identified.

Audit Response. The documentation and additional clarification provided by DTRA supported the assertion that the interfaces already identified by the auditors had been tested. Additionally, we accept the Program Manager's attestation that there were no additional interfaces.

4. Include the Compliance Monitoring and Tracking System in appropriate higher level testing;

Management Comments. The DTRA stated, in response to the draft report, that the end-to-end testing of CMTS in September 1999 included all interfaces identified by the auditors. The DTRA maintained that the Argonne National Laboratory (Argonne) testing in March met the higher level testing requirement. However, they redid portions of the test in September to capture screen prints and other hard copy documentation not previously provided to the DoDIG auditors. DTRA maintained that CMTS was a stand-alone system in that only data identified in the response was imported and no data was exported to other systems.

Audit Response. The CMTS is not a stand-alone system because it imports data; however, CMTS is unique in that none of its interfaces is mission critical. Therefore, there was no mission critical thread to be tested in end-to-end testing. The additional documentation provided by DTRA showed that it met the end-to-end testing requirement.

5. Recertify the Compliance Monitoring and Tracking System at the appropriate level.

Management Comments. The DTRA maintained that CMTS was appropriately certified. Because the documentation did not clearly show the two levels of testing required for a level 1a certification, DTRA provided additional documentation to show that the contractor (TRW) conducted it's own testing while developing the software, which constitutes the first level of testing. The second level was done independently by Argonne with the TRW contractor personnel present to answer questions. The DTRA pointed out that a June 15, 1999 letter from Argonne to DTRA clearly shows that Argonne developed the test plans and performed the March testing.

Audit Response. DTRA provided the contractor statement of work showing the contractor's (TRW) Y2K testing and the intent to have a third-party contractor perform independent testing. These two levels of testing meet the level 1 certification requirement. Additionally, the statement of work showed that the contractor would be converting 2-digit date fields to 4-digit date fields, which supports the "a" portion of the 1a certification.

Appendix A. Audit Process

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 DoD efforts to address the Y2K computing challenge. For a listing of audit projects addressing the issue, see the Y2K webpage on the IGnet at http://www.ignet.gov.

Scope

CMTS Review. To assign a system risk, we reviewed and evaluated the CMTS testing. The Technical Assessment Division, Office of the Inspector General, DoD, reviewed the CMTS test plan and test results to determine whether the system had been adequately tested. We compared the Y2K efforts of testing and certifying CMTS with the requirements in the DoD Management Plan. We also reviewed the CMTS contingency plans and compared them to the DoD Management Plan requirements.

DoD-Wide Corporate-Level Government Performance and Results Act (GPRA) Goals. In response to the GPRA, the Department of Defense has established 2 DoD-wide goals and 7 subordinate performance goals. This report pertains to achievement of the following goals (and subordinate performance goals):

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

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following 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)**
- **Objective:** Provide services that satisfy customer information needs.
  Goal: Modernize and integrate Defense information infrastructure. **(ITM-2.2)**
- **Objective:** Provide services that satisfy customer information needs.
  Goal: Upgrade technology base. **(ITM-2.3)**

General Accounting Office 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 the problem and of the overall Information Management and Technology high-risk area.

Methodology

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

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

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

Appendix B. Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Inspector General, DoD, reports can be accessed over the Internet at http://www.dodig.osd.mil/. The Inspector General, DoD, issued the following Y2K reports relating to the Defense Threat Reduction Agency.

Inspector General, DoD, Report No. 99-252, "Year 2000 Status of the Centralized Accounting and Financial Resource Management System, Defense Threat Reduction Agency" September 15, 1999. The report states that the Centralized Accounting and Financial Resource Management System was not planned for inclusion in any type of higher level testing as required by the DoD Management Plan for all mission-critical systems that are date dependent and are not operating in a stand-alone environment. The DTRA initially maintained that the Centralized Accounting and Financial Resource Management System was essentially a stand-alone system and therefore not subject to the requirement for a higher level test. However, the Centralized Accounting and Financial Resource Management System is not a stand-alone system because it has external interfaces with other DoD financial systems. During the course of the audit, DTRA developed a new action plan for the implementation, testing, and recertification of the Centralized Accounting and Financial Resource Management System to include higher level testing as required by the DoD Management Plan. The report states that the risk that the Centralized Accounting and Financial Resource Management System will fail or have an adverse impact on other DoD financial systems due to Y2K-related events will be reduced if the new action plan is successfully implemented. The report recommended that the Comptroller, Defense Threat Reduction Agency, verify that the Centralized Accounting and Financial Resource Management System Action Plan is completed timely and fulfills the testing requirements of the DoD Management Plan.

Inspector General, DoD, Report No. 99-235, "Year 2000 Status of the Defense Threat Reduction Agency Nuclear Weapon Status Information Systems," August 19, 1999. The report states that DTRA exercised due diligence in validating the Y2K readiness of its mission-critical Nuclear Weapon Information Tracking Systems. Specifically, for the Nuclear Management Information System, the Nuclear Weapons Contingency Operations Module, and the Special Weapons Information Management System, DTRA assessed the Y2K compliance of the system inventory; conducted Y2K system verification and certification testing; assessed the system interfaces; developed and tested its system contingency plans; participated in the first of two required operational readiness tests; and scheduled a second operational readiness test. As a result, DTRA obtained a reasonable level of assurance that the functions performed by the Nuclear Management Information System, the Nuclear Weapons Contingency Operations Module, and the Special Weapons Information Management System will continue after the year 2000.

Inspector General, DoD, Report No. 99-234, "Year 2000 Status of the Nuclear Inventory Management and Cataloging System," August 19, 1999. The report states that DTRA, Albuquerque Operations, adequately assessed Y2K issues to ensure Y2K compliance of the Nuclear Inventory Management and Cataloging System, but did not fully document all relevant information that should have been included as the basis of Y2K certification. The Nuclear Inventory Management and Cataloging System inventory did not show the version of the product used; the test plan and report did not adequately describe test procedures, expected results, and actual results; the contingency plan was not practical; and the level of certification was incorrect. The report states that initial errors in the System and Operational Contingency Plan were corrected.

The report recommended that the Chief Information Officer, DTRA, provide active ongoing oversight of the Nuclear Inventory Management and Cataloging System to include the completion of the following: update and maintain the Nuclear Inventory Management and Cataloging System inventory, test plan, and certification checklist; revise the Office of the Secretary of Defense Y2K database to reflect the appropriate certification level; update the contingency plan; and verify the Y2K compliance of the equipment requirements for the backup server when conducting the contingency plan test.

The DTRA provided information subsequent to the draft report that was a significant improvement and that included necessary information as the basis of Y2K certification. Also, DTRA provided an After Action Plan of the lessons learned, a Test Analysis Report, and an updated Nuclear Inventory Management and Cataloging System and Operational Contingency Plan.

Inspector General, DoD, Report No. 99-034, "Management of the On-Site Inspection Agency Year 2000 Program," November 12, 1998.

Inspector General, DoD, Report No. 99-030, "Management of the Defense Technology Security Administration Year 2000 Program," November 3, 1998.

Inspector General, DoD, Report No. 99-028, "Management of the Defense Special Weapons Agency Year 2000 Program," October 30, 1998.

Appendix C. Report Distribution

Office of the Secretary of Defense

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

Joint Staff

Director, Joint Staff

Department of the Army

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
Inspector General, Marine Corps

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

Unified Commands

Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Joint Forces Command
Commander in Chief, U.S. Southern Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. Space Command
Commander in Chief, U.S. Special Operations Command
Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command

Other 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, Defense Threat Reduction Agency
  Chief Information Officer, Defense Threat Reduction Agency
  Inspector General, Defense Threat Reduction Agency
  Commander, Defense Threat Reduction Agency, Albuquerque Field Operations

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
  Director, Defense Information and Financial Management Systems, Accounting and Information Management Division, General Accounting Office

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

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (con't)

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

Defense Threat Reduction Agency Comments

Defense Threat Reduction Agency
45045 Aviation Drive
Dulles, VA 20166-7517

OCT 12 1999

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

Subject: Response to Audit Report on Year 2000 Status of Compliance Monitoring and Tracking System (Project No. 9AS-0090.08)

Reference is made to your audit report of the same subject, dated September 27, 1999, which provided one summary recommendation. The Defense Threat Reduction Agency (DTRA) has reviewed the summary of recommendations and has the following comments.

Results: The ability of the Compliance Monitoring and Tracking System (CMTS) to operate successfully in the year 2000 may be impaired because the DTRA did not appropriately certify the CMTS. Specifically, the DTRA did not identify all system interfaces, obtain necessary interface agreements, include all interfaces in system-level testing or include CMTS in appropriate higher level testing. Additionally, testing documentation did not support the certification level reported by the DTRA. Although contingency plans have been developed and tested, it would be preferable to complete the actions necessary to ensure system compliance so that chances of system failures are minimized.

Summary of Recommendations: We recommend that the Director, DTRA, identify all systems that interface with the CMTS; obtain interface agreements, including all requirements outlined in the DoD Y2K Management Plan, for each of those interfaces, test all interfaces as part of system-level testing; include the CMTS in appropriate higher level testing; and re-certify the CMTS at the appropriate level.

DTRA Response:

a. Identify all systems that interface with the CMTS. TIIMS, SPARTANS and Air Force and Army data imports have been identified as interfaces to CMTS. In response to the DoDIG proposed draft audit report, September 1999, all supporting documentation for SPARTANS, Air Force and Army imports was

obtained and provided to the DoDIG on September 21, 1999. TIIMS was identified by DTRA as an interface in March 1999, and documentation was provided at that time. Interface documentation is also attached with this response. Also provided is a letter signed by the CMTS Program Manager certifying that no other interfaces to CMTS exist. A document entitled "Functional End-to-End Testing (E2E) of the Processes of the Compliance Monitoring and Tracking System" is also attached to provide supplemental information regarding identification, testing and test results of interfaces.

b. Obtain Interface Agreements. In response to the DoDIG proposed draft audit report, September 1999, interface agreements for SPARTANS, Air Force and Army were obtained and provided to the DoDIG as received by DTRA between 21 and 23 September 1999. Those interface agreements are provided as an attachment to this response.

c. Test all interfaces as part of system-level testing. All interfaces were tested during the 6-26 March 1999, system testing. However, documentation was not provided as SPARTANS, Air Force and Army data imports were not identified as interfaces until August 1999. To substantiate that the interfaces were part of system-level testing, reference is made to the attached document entitled "The Compliance Monitoring and Tracking System Windows NT Functional Test Plan", dated February 26, 1999. This document was provided to the DoDIG on April 5, 1999, during their first visit to DTRA and again on September 21, 1999. Reference page 5, Table 1, CMTS Functions and Utilities to be Tested in the Functional Test. At Table 1, Notification Processing, Generation - SCDS, "import" is listed as a task. This refers to the SPARTANS data. Also, at Table 1, DMRS Functions, the first task is "import data" and this refers to the Air Force and Army data. Also, reference is made to the same attachment, page 11, second full paragraph, "In SCDS, the Navy must be able to import START and START II notifications created in their SPARTANS." Also, reference page 20, paragraph 4.4.1 "this set of tests will demonstrate that DMRS can import data from external data sources". Data was imported into the CMTS from diskettes as part of the March 1999, independent validation and verification testing performed by Argonne National Labs.

The DODIG identified SPARTANS, Air Force and Army data as interfaces in August 1999, and reported these findings in their proposed draft audit report, September 1999. In response to this report, DTRA conducted end-to-end testing of the three

interfaces. Diskettes from SPARTANS, Air Force and Army were obtained, imported into CMTS, screen prints captured of each step in the process and screen prints captured of the data within CMTS. All documentation was provided to the DoDIG on September 21, 1999 and is again provided as an attachment to this response. Only the SPARTANS data contains four-digit year date fields. No date fields are contained in the Air Force and Army data. Upon import into CMTS, an embedded application within CMTS, checks all data for compliance to treaty specified formats, to include date formats. No errors were received during the testing for any import.

DTRA is confident in the ability of CMTS to operate successfully in the year 2000. Data imported from Navy, Air Force and Army interfaces is imported annually and is used as a comparison aid by the services to reconcile anomalies in service maintained data external to CMTS. The CMTS is the official U.S. national system employed to satisfy treaty and agreement reporting requirements and is the only official data source used to satisfy annual exchanges of data. This data exchange is by way of paper copy hand carried to Vienna, Austria. No electronic exchange occurs. Because CMTS contains the U.S. official data, it is in no way dependent upon imported data from external sources to meet any reporting obligations; the data already resides within CMTS. Again, the only reason for the imports is to assist the services in reconciling their numbers against official numbers contained in the CMTS database. In the event of a system/process failure on the interface side, CMTS would not require the annual import of data in order to meet reporting obligations. CMTS would be in no way affected by a failure of any interface.

d. Include the CMTS in appropriate higher level testing. The CMTS higher level testing has been satisfied as demonstrated in the attached document entitled "Functional End-to-End Testing (E2E) of the Processes of the Compliance Monitoring and Tracking System (CMTS)". Again referring to the attached document entitled "Compliance Monitoring and Tracking System (CMTS) Windows NT Functional Test Plan", dated February 26, 1999, the plan substantiates that the import processes were part of the system testing.

CMTS is a stand-alone system in that only data identified herein is imported but no data is exported to other systems nor is there any type of recurring exchange of data between CMTS and other systems.

e. Re-certify the CMTS at the appropriate level. Clarification on this issue was received during a telephone conversation on October 7, 1999 between DoDIG staff and CMTS staff. DTRA, with concurrence of the DoDIG, has demonstrated and is confident that the required two levels of testing have been satisfied, based on clarification of the requirement during the referenced telephone conversation. The DoDIG did not see any reference in the test documentation referring to two (2) levels of testing, and therefore, concluded that the first level of testing was conducted in March 1999, by independent validation and verification (IV&V) agent, Argonne National Labs. However, two levels of testing were satisfied, the first of which was conducted by TRW, Inc., as the CMTS software developer. Per a statement of work issued in February 1998, TRW, Inc., began the conversion of CMTS software from Windows 3.1 to the Windows New Technology (NT) operating system. This effort also included making all necessary date changes to bring CMTS software to a Y2K compliant level. As this reprogramming was performed, TRW, Inc., performed on a regular basis, unit and system testing. This is a necessity of any programming effort in order for the contractor to verify that reprogramming results in an expected outcome. At the direction of the CMTS Program Manager, the CMTS software baseline was frozen on March 6, 1999 the first day of IV&V testing. At that time, TRW, Inc. turned over for IV&V what they believed was a Y2K compliant system. This same day the TRW, Inc., programming effort ended and the Argonne National Labs IV&V effort began. Argonne National Labs, under direction of the CMTS Program Manager, developed, executed and analyzed all aspects of the IV&V to include test plans, test scenarios, execution of testing and results reporting. There was no collaboration between TRW, Inc., and Argonne National Labs. Argonne National Labs does not have access to the CMTS software until their arrival in the test lab the day testing begins.

The IV&V testing was conducted by Argonne National labs at the CMTS test lab with the TRW program manager and lead programmer available in order to respond to any programming anomalies identified by testers. TRW personnel did not participate in the execution of test.

Documentation provided to the DoDIG included a funding package to Argonne National Labs (package attached). The IACRO (DTRA Form 48) stated the execution work unit title as "CMTS Windows NT/Y2K Conversion" and this mislead the DoDIG. This statement should have indicated work to be performed as IV&V testing; however, all other funding documentation (such as the

Statement of Work) states that the purpose of Argonne National Labs activities was to perform IV&V testing of CMTS. During the October 7, 1999 phone conversation, the DoDIG did state that the June 15, 1999 letter (attached) from Argonne National Labs certifying CMTS as Y2K compliant, is accepted as verification that Argonne National Labs was not involved in any development and serves to clarify any misrepresentation on the IACRO. Therefore, DTRA does not believe that re-certification of CMTS is necessary.

DTRA appreciates the opportunity to comment on the draft report. Please express our appreciation to your staff for their hard work in helping us prepare for Y2K. Please address any questions or comments to Capt Richard Towner, DTRA Chief of Staff and Acting Chief Information Officer at 703-810-4178.

Richard L. Towner for

Jay Davis
Director

Attachments:
CMTS Year 2000 Interface Documentation
Compliance Monitoring and Tracking System (CMTS) Functional Test Plan, February 26, 1999
Functional End-to-End (E2E) of the Processes Compliance Monitoring and Tracking System (CMTS)
DTRA/ANL Funding Package
Letter, subject Year 2000 Compliance of the Compliance Monitoring and Tracking System (CMTS) Version 2.0 - certification of compliance by Argonne National Labs
Letter, dated October 12, 1999, signed by Antwane Johnson certifying that all interfaces have been identified

-5-

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
Mary Lu Ugone
Kathryn M. Truex
Amy L. Schultz
Krista S. Gordon