Audit Report

MANAGEMENT OF THE ON-SITE INSPECTION AGENCY
YEAR 2000 PRORAM

Report No. 99-034 November 12, 1998

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 Analysis, Planning, 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 Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) or FAX (703) 604-8932 Ideas and requests can also be mailed to

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

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-8908, 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

OSIA	On-Site Inspection Agency
Y2K	Year 2000

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

November 12, 1998

MEMORANDUM FOR DIRECTOR, DEFENSE THREAT REDUCTION AGENCY

SUBJECT Audit Report on Management of the On-Site Inspection Agency Year 2000 Program (Report No 99-034)

We are providing this audit report for your information and use

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

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Mary Lu Ugone at (703) 604-9049 (DSN 664-9049), <email mlugone@dodig.osd.mil>, Ms Kathryn M Truex at (703) 604-9045 (DSN 664-9045), <email kmtruex@dodig.osd mil>, or Ms Kathleen M. Fitzpatrick at (410) 859-6995 <email kmfitzpatric@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. 99-034 **November 12, 1998**
(Project No 8AS-0032.04)

Management of the On-Site Inspection Agency Year 2000 Program

Executive Summary

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

Information technology systems have typically used two digits to represent the year, such as "98" representing 1998, to conserve electronic storage and to reduce operating costs With the two-digit format, however, the year 2000 is indistinguishable from 1900 As a result of the ambiguity, computers and associated systems and application programs that use dates to calculate, compare, and sort could generate incorrect results when working with years after 1999

Audit Objective. The overall audit objective was to determine whether planning and management within the On-Site Inspection Agency were adequate to ensure that continuity of operations is not unduly disrupted by year 2000 issues.

Audit Results. The On-Site Inspection Agency has recognized the importance of the year 2000 issue and has taken positive actions in addressing the year 2000 problem The progress that the On-Site Inspection Agency made in resolving the year 2000 computing issue is not complete Unless the On-Site Inspection Agency makes further progress on mitigating year 2000 risks, the On-Site Inspection Agency, as a part of the Defense Threat Reduction Agency, may be unable to fully execute its mission without undue disruptions See Part I for details of the audit results

Summary of Recommendations. We recommend that the Director, On-Site Inspection Agency, implement revisions from the "DoD Year 2000 Management Plan, For Signature Draft Version 2.0"; document changes in the status of systems; update the contingency plan for its mission-critical system; develop plans for any other system, the failure of which may cause disruptions to its mission, document the testing methodology to show how systems are determined to be compliant; update the continuity-of-operations plan to address the year 2000 issue, and continue taking a proactive stance with regard to sector outreach

Management Comments. The Director, On-Site Inspection Agency, concurred with the recommendations See Part I for a summary of management comments and Part III for the complete text of the comments.

Table of Contents

Executive Summary i

Part I - Audit Results

Audit Background 2
Audit Objective 4
Status of the On-Site Inspection Agency Year 2000 Program 5

Part II - Additional Information

Appendix A Audit Process
Scope 12
Methodology 13
Prior Audit Coverage 13
Appendix B. Report Distribution 14

Part III - Management Comments

On-Site Inspection Agency Comments 18

Part I - Audit Results

Audit Background

The year 2000 (Y2K) problem is the term most often used to describe the potential failure of information technology systems to process or perform date-related functions before, on, or after the turn of the century The Y2K problem is rooted in the way that automated information systems record and compute dates For the past several decades, systems have typically used two digits to represent the year, such as "98" representing 1998, to conserve on electronic data storage and reduce operating costs With the two-digit format, however, 2000 is indistinguishable from 1900 As a result of the ambiguity, computers and associated system and application programs that use dates to calculate, compare, or sort could generate incorrect results when working with years following 1999. Calculation of Y2K dates is further complicated because the Y2K is a leap year, the first century leap year since 1600. The computer systems and applications must recognize February 29, 2000, as a valid date

Because of the potential failure of computers to run or function throughout the Government, the President issued an Executive Order, "Year 2000 Conversion," February 4, 1998, making it policy that Federal agencies ensure that no critical Federal program experiences disruption because of the Y2K problem The Executive Order also requires that the head of each agency ensure that efforts to address the Y2K problem receive the highest priority attention in the agency.

DoD Y2K Management Strategy. In his role as the DoD Chief Information Officer, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued the "DoD Year 2000 Management Plan" (DoD Management Plan) in April 1997 The DoD Management Plan provides the overall DoD strategy and guidance for inventorying, prioritizing, fixing, or retiring systems, and monitoring progress. The DoD Management Plan states that the DoD Chief Information Officer has overall responsibility for overseeing the DoD solution to the Y2K problem Also, the DoD Management Plan makes the DoD Components responsible for implementing the five-phase Y2K management process The "DoD Year 2000 Management Plan, For Signature Draft Version 2 0" (Draft DoD Management Plan), June 1998, accelerates the target completion dates for the renovation, validation, and implementation phases. The new target completion date for implementation of mission-critical systems is December 31, 1998, and for non-mission-critical systems is March 31, 1999.

In a memorandum dated January 20, 1998, for the heads of executive departments and agencies, the Office of Management and Budget established a new target date of March 1999 for implementing corrective actions to all systems. The new target completion dates are September 1998 for the renovation phase and January 1999 for the validation phase

The Secretary of Defense issued a memorandum "Year 2000 Compliance" on August 7, 1998, which stated that DoD progress in addressing the Y2K computer problem was insufficient He directed that Defense agencies will be responsible for

ensuring that the list of mission-critical systems under their respective purview is accurately reported in the DoD Y2K database effective October 1, 1998. Defense agencies must report and explain each change in mission-critical designation to the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) within 1 month of the change.

The Deputy Secretary of Defense issued the memorandum "Year 2000 (Y2K) Verification of National Security Capabilities" on August 24, 1998. The memorandum states that each of the Directors of the Defense Agencies must certify that they have tested the information technology and national security system Y2K capabilities of their respective component's systems in accordance with the DoD Management Plan

On-Site Inspection Agency. The On-Site Inspection Agency (OSIA) was established on January 15, 1988, after the United States and Russia (formerly the Soviet Union) signed the Intermediate-Range Nuclear Forces Treaty, the first arms control agreement to mandate the destruction of an entire class of nuclear missiles, on December 8, 1987

OSIA conducts U S Government inspections of foreign facilities, units, territories, or events under the provisions of arms control treaties and agreements and coordinates foreign inspections of analogous U S facilities, units, territories, or events. To accomplish its mission, OSIA.

- organizes, trains, equips, deploys, and exercises operational control over inspection, monitoring, escort, and observation teams to ensure that the U.S Government can exercise its full treaty rights for on-site inspection and to protect U S treaty rights with respect to inspected sites or activities,

- provides technical advice to U.S. Government elements concerned with developing, implementing, or evaluating compliance with arms control treaties and agreements; and

- executes other missions requiring unique skills, organization, or experience resident in OSIA

Defense Threat Reduction Agency. Under the auspices of the Defense Reform Initiative, OSIA merged with the Defense Special Weapons Agency, the Defense Technology Security Administration, and some program functions of the Assistant to the Secretary of Defense (Nuclear, Chemical, and Biological Defense Programs). The Defense Threat Reduction Agency, which began operations on October 1, 1998, is the focal point of DoD for addressing proliferation of weapons of mass destruction

The Defense Threat Reduction Agency's mission is to reduce the threat to the United States and its allies from nuclear, biological, chemical, conventional, and special weapons through the execution of technology security activities; cooperative threat reduction programs; arms control treaty monitoring and on-site

inspection, force protection; nuclear, biological, and chemical defense, and counter-proliferation to support the U.S nuclear deterrent and to provide technical support on weapons of mass destruction matters to DoD Components.

Audit Objective

The overall audit objective was to determine whether planning and management within OSIA were adequate to ensure that continuity of operations is not unduly disrupted by year 2000 issues. See Appendix A for a discussion of the audit scope, methodology, and prior audit coverage

Status of the On-Site Inspection Agency Year 2000 Program

The OSIA has recognized the importance of the Y2K issue and has taken positive actions to address the Y2K problem However, the progress is not complete because OSIA has not completed all the actions necessary to minimize the adverse impact of Y2K date processing on its mission-critical and non-mission-critical systems Specifically, OSIA did not·

- update the OSIA draft Y2K management plan to reflect the latest changes in the Draft DoD Management Plan,

- update the contingency plan for its mission-critical system and develop contingency plans for any other system the failure of which may cause disruption to the mission of OSIA,

- document testing methodology for systems identified as Y2K compliant,

- include Y2K issues in its continuity-of-operations plan for the mission of OSIA as a part of the Defense Threat Reduction Agency, and

- take a proactive stance with regard to sector outreach.

Unless OSIA makes further progress on mitigating Y2K risks, OSIA, as a part of the Defense Threat Reduction Agency, may not be able to fully execute its mission without undue disruptions.

Actions Taken to Address the Year 2000 Problem

The OSIA has taken the following actions as part of its efforts to address the Y2K problem·

- appointed a Y2K point of contact,

- prepared an OSIA draft Y2K management plan,

- included Y2K compliance language in all new contracts and contract modifications contracts,

- attended DoD Y2K interface assessment workshop meetings and established working relationships with other DoD system owners, and

- began replacing personal computers and operating systems that are not Y2K compliant

OSIA Draft Y2K Management Plan

Management Plan. The OSIA draft Y2K management plan is intended to provide the roles, responsibilities, timelines, and guidelines for OSIA Y2K problem-resolution efforts

The OSIA tailored its draft management plan to the DoD Management Plan and intended for it to address the Y2K problem by implementing the five phases that the DoD Management Plan requires However, the plan does not require OSIA to monitor and update its plan based on changes to the Draft DoD Management Plan as well as guidance from the Secretary of Defense, the Office of Management and Budget, and the President's Council on Year 2000 Conversion

Mission-Critical System. OSIA had identified two mission-critical systems· the Compliance Monitoring and Tracking System and the Treaty Inspection and Information Management System; both systems support U S. Government treaties During the audit, OSIA reassessed the Treaty Inspection and Information Management System and changed its status from mission-critical to non-mission-critical because its mission-critical functions have been incorporated into the Compliance Monitoring and Tracking System OSIA should document the change in status and the basis for that change.

Contingency Plans

The OSIA has a security concept-of-operations plan that contains a contingency planning section for system failure for its mission-critical system, the Compliance Monitoring and Tracking System, which was scheduled to finish testing in April 1999 In accordance with the Draft DoD Management Plan, OSIA should update the contingency plan to include Y2K contingencies Also, the contingency plan should address the risk that Y2K disruptions may also affect back-up and alternate systems.

The Draft DoD Management Plan states that to adequately plan for Y2K disruptions, DoD Components must ensure that Y2K contingency plans address a wide range of workarounds that will enable the component to carry out its mission The plan should include "back to basics" approaches that may be necessary to sustain mission-critical capabilities.

OSIA said that it would update the contingency plan for its mission-critical system, the Compliance Monitoring and Tracking System, to address Y2K issues and complete the plan by December 1998 In accordance with the Draft DoD Management Plan, OSIA should also assess its non-mission-critical systems to determine whether contingency plans are needed and develop contingency plans for any other system the failure of which may cause disruptions to the functions of OSIA.

Compliance Certification and Testing

Compliance Certification. The Draft DoD Management Plan requires that the system developers and maintainers, along with the system's functional proponent, certify and document each system's Y2K compliance System certification requires signatures by the system manager, the project manager, and the customer on the compliance checklist confirming completion of testing in accordance with the Draft DoD Management Plan OSIA should retain the signed checklist as part of the system documentation An example of a Y2K compliance checklist is in Appendix G of the Draft DoD Management Plan

Inspector General, DoD, Report No 98-147, "Year 2000 Certification of Mission-Critical DoD Information Technology Systems," June 5, 1998, states that DoD Components were not complying with Y2K certification criteria before reporting systems as compliant Of the 430 systems that DoD reported as Y2K compliant in November 1997, the report estimates that DoD Components certified only 109 systems (25.3 percent) as Y2K compliant. As a result, DoD management reported as Y2K compliant systems that had not been certified More important, mission-critical DoD information technology systems may unexpectedly fail because they were classified as Y2K compliant without adequate basis. The results were based on a randomly selected sample of 87 systems that DoD had reported as Y2K compliant

OSIA Compliance Certification. The mission-critical system of OSIA, the Compliance Monitoring and Tracking System, which was scheduled to finish testing in April 1999, had not been reported as compliant. OSIA said that it would complete a Y2K compliance certification checklist for the system before reporting to DoD that the system is compliant

OSIA had reported to DoD its once mission-critical system, the Treaty Inspection and Information Management System, as compliant but had not completed a Y2K compliance checklist for the system.

OSIA identified more than 20 non-mission-critical systems as compliant, but it did not document the basis for determining the systems as compliant. OSIA should not identify any of its systems as compliant until it documents the Y2K compliance A checklist could be one way for OSIA to document its Y2K testing methodology.

Testing. The Draft DoD Management Plan states that DoD Components not only must test for Y2K compliance of individual applications, but must test the complex interactions between scores of converted or replaced computer platforms, operating systems, utilities, applications, databases, and interfaces Renovated systems must also be tested for any new software bugs introduced while fixing Y2K problems OSIA identified more than 20 non-mission-critical systems as compliant, but did not document the Y2K testing methodology that it relied upon to determine compliance.

The Draft DoD Management Plan suggests that DoD Components test all commercial off-the-shelf and Government off-the-shelf products for Y2K

compliance before installation when that particular product is not listed in the General Services Administration home page as being Y2K compliant OSIA should document its Y2K testing methodology, including its off-the-shelf products

Continuity-of-Operations Plan

The Draft DoD Management Plan states that DoD Components are responsible for developing a Component continuity-of-operations plan. The plan should include a prioritized list of systems and major actions taken to minimize Y2K disruption. OSIA had a continuity-of-operations plan, but the plan did not address Y2K issues for the mission of the On-Site Inspection Agency as a part of the Defense Threat Reduction Agency

Sector Outreach

The President's Council on Year 2000 Conversion issued a draft "Sector Analysis for DoD Support" (Sector Analysis) dated June 11, 1998 The Sector Analysis assigns sectors of the Federal Government, such as Defense, telecommunications, and education, to "lead Federal agencies" to coordinate, plan, and lead execution of Y2K actions across all other agencies Areas of interest that the Sector Analysis assigned to DoD as the lead Federal agency included the following·

- Defense treaties and alliances,
- Defense treaty obligations, and
- Defense coalitions and mutual support agreements

At the beginning of the audit, OSIA said that it was not aware of the Sector Analysis and that none of the areas applied to OSIA However, OSIA had since started taking a proactive stance with regard to Sector Analysis, both domestically and internationally, for the Defense Threat Reduction Agency mission.

Conclusion

The OSIA recognized the importance of solving Y2K problems in systems to reduce the risk of Y2K failure, but OSIA must take a more aggressive approach in documenting and testing for Y2K compliance for all of its systems and off-the-shelf products. OSIA must continually monitor and assess the progress of Y2K compliance, update contingency plans, and document testing of systems In addition, OSIA must update its continuity-of-operations plan to specifically address the Y2K issue and continue a proactive stance with regard to sector outreach for the Defense Threat Reduction Agency mission.

Recommendations and Management Comments

We recommend that the Director, On-Site Inspection Agency:

1. Implement the revisions from the "DoD Year 2000 Management Plan, For Signature Draft Version 2.0" and other Department of Defense and Presidential guidance and integrate that guidance into the On-Site Inspection Agency year 2000 management plan.

2. Document changes in year 2000 status and the basis for the change for On-Site Inspection Agency systems.

3. Update the contingency plan for its mission-critical system to include year 2000 contingencies and develop contingency plans for any other system the failure of which may cause disruptions to the mission of the On-Site Inspection Agency, in accordance with the "DoD Year 2000 Management Plan, For Signature Draft Version 2.0."

4. Document the year 2000 testing methodology for determining year 2000 compliance of systems.

5. Update the continuity-of-operations plan to specifically address the year 2000 issues and the mission of the On-Site Inspection Agency as a part of the Defense Threat Reduction Agency.

6. Continue taking a proactive stance with regard to sector outreach, both domestically and internationally, for the Defense Threat Reduction Agency mission.

Management Comments. OSIA concurred with all of the recommendations, stating progress made and future intentions for each recommendation. Management stated that it will review DoD and Presidential Y2K guidance and update the OSIA Y2K management plan appropriately Management will also include the process for documenting changes in the Y2K status of systems and include the requirement for documentation of testing methods in the OSIA Y2K management plan. Additionally, management will update both contingency plans and the continuity-of-operations plan to include Y2K issues Finally, management will formalize and document sector outreach involvement

Part II - Additional Information

Appendix A. Audit Process

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

Scope

We reviewed the status of the progress of OSIA in resolving the Y2K computing issue We evaluated the Y2K efforts of OSIA, compared with those efforts described in the DoD Management Plan issued by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in April 1997. We obtained documentation including the draft OSIA Y2K management plan and systems inventory status information as of June 1998 We used the information to assess efforts related to the multiple phases of managing the Y2K problem.

DoD-Wide Corporate-Level Government Performance and Results Act 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 warfighting capabilities **(DoD-3)**

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

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from June through August 1998 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 the 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 1997 Annual Statement of Assurance

Prior Audit Coverage

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

Appendix B. 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)
  Year 2000 Oversight and Contingency Planning Office
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

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
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

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
  Chief Information Officer
  Inspector General
  United Kingdom Liaison Officer
Director, Defense Logistics Agency
Director, Defense Threat Reduction Agency
  Inspector General, Defense Threat Reduction 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

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

Chairman and ranking minority member of each of the following congressional committees and subcommittees:

  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 National Security, Committee on Appropriations
  House Committee on Government Reform and Oversight
  House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and Oversight
  House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform and Oversight
  House Committee on National Security

Part III - Management Comments

On-Site Inspection Agency Comments

ON-SITE INSPECTION AGENCY
PO BOX 17498
WASHINGTON DC 20041-0498

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Response to Audit Report on Management of the On-Site Inspection Agency (OSIA) Year 2000 Program (Project No. 8AS-0032.04)

We have reviewed the draft Audit Report on Management of the OSIA Year 2000 Program and provide the following comments:

a We concur with the finding of the draft audit report

b. We concur with all of the recommendations for corrective actions, specifically:

(1) The need to implement revisions from the "DoD Year 2000 Management Plan, for Signature Draft Version 2.0" and other DoD and Presidential guidance and to integrate that guidance into the OSIA Year 2000 management plan.

(2) The need to document changes in year 2000 status and document the basis for that change for OSIA systems

(3) The need to update the contingency plan for the Compliance Monitoring and Tracking System (CMTS) to include year 2000 contingencies and to develop contingency plans for any other system the failure of which may cause disruptions to the mission of the OSIA, in accordance with the "DoD Year 2000 Management Plan, For Signature Draft Version 2 0."

(4) The need to document the year 2000 testing methodology for determining year 2000 compliance of systems.

(5) The need to update the continuity-of-operations plan to specifically address the year 2000 issues and the mission of the OSIA as a part of the Defense Threat Reduction Agency.

(6) The need to continue taking a proactive stance with regard to sector outreach, both domestically and internationally, for the Defense Threat Reduction Agency.

The point of contact for this action is Capt Allan Toole at 703-326-8611.

Joerg H. Menzel
Acting Director

Attachment:
As stated

SCHEDULE OF PLANNED Y2K ACTIONS

Recommended Correction	Planned Actions	Completion Date
Integrate DoD and Presidential Y2K Guidance into OSIA Y2K management plan	1) Review DoD Y2K Management Plan, ver 2.0 2) Review other DoD and Presidential guidelines 3) Review existing OSIA Y2K Management Plan 4) Update OSIA Y2K Management Plan appropriately	16 Oct 98
Document changes in Y2K status and document the basis for that change for OSIA systems	1) Include in OSIA Y2K Management Plan the process for documenting changes in Y2K status of systems 2) Implement process with issuance of management plan	16 Oct 98 (process implentation date, then on-going)
Update contingency plan for CMTS and create other system contingency plans as necessary regarding Y2K	1) Update contingency plan for CMTS 2) Identify and create/update contingency plans for other systems	31 Dec 98
Document Y2K testing methodology for determining Y2K compliance	1) Include requirement for documentation of testing method in OSIA Y2K Management Plan 2) Implement process with issuance of management plan	16 Oct 98 (process implementation date, then on-going)
Update COOP to address Y2K issues and the OSIA mission as part of DTRA	1) Update COOP to address Y2K issues and the OSIA mission as part of DTRA	31 Dec 98
Continue sector outreach involvement, domestically and internationally, for DTRA	1) Formalize and document sector outreach involvement	Implemented;on-going

Audit Team Members

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

Thomas F Gimble
Patricia A. Brannin
Mary Lu Ugone
Kathryn M Truex
Kathleen M. Fitzpatrick
Jennifer L Zucal