Audit Report

MANAGEMENT OF THE DEFENSE TECHNOLOGY SECURITY ADMINISTRATION YEAR 2000 PROGRAM

Report No. 99-030 November 3, 1998

Office of the Inspector General
Department of Defense

19990908 016

DTIC QUALITY INSPECTED 4

AQI 99-12-2279

Additional Information and 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 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, 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

DTSA	Defense Technology Security Administration
Y2K	Year 2000

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

November 3, 1998

MEMORANDUM FOR DIRECTOR, DEFENSE THREAT REDUCTION AGENCY

SUBJECT Audit Report on Management of the Defense Technology Security Administration Year 2000 Program (Report No 99-030)

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

Management comments conformed to the requirements of DoD Directive 7650 3 The Director, Defense Technology Security Administration, concurred with the recommendations

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) (mlugone@dodig osd mil), Ms Kathryn M Truex at (703) 604-9045 (DSN 664-9045) (kmtruex@dodig osd mil), or Ms. Virginia G Rogers at (703) 604-9041 (DSN 664-9041) (vrogers@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. 99-030 **November 3, 1998**
(Project No. 8AS-0032 05)

Management of the Defense Technology Security Administration Year 2000 Program

Executive Summary

Introduction. This is one of 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 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.

Objectives. Our overall objective was to determine whether planning and management within the Defense Technology Security Administration were adequate to ensure that continuity of operations will not be unduly disrupted by year 2000 related issues. Specifically, the audit addressed the actions taken by the Defense Technology Security Administration to resolve date-processing issues regarding the year 2000, as well as preparation of plans to address year 2000 related system failures that could impact the ability of the Defense Threat Reduction Agency to perform its mission

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

Summary of Recommendations. We recommend that the Director, Defense Technology Security Administration, report systems as compliant after completing year 2000 compliance checklists, submit quarterly reports as required, develop contingency plans as appropriate, develop a continuity-of-operations plan to specifically address the year 2000 issue, assume a proactive stance with regard to sector outreach, and implement the DoD Year 2000 Management Plan and its revisions and other DoD and Presidential guidance

Management Comments. The Director, Defense Technology Security Administration, concurred with the recommendations, stating that management has developed a compliance checklist and is currently testing components. Management is also preparing quarterly reports. Under the Defense Threat Reduction Agency, contingency plans will be developed and the continuity-of-operations plan will be updated to address year 2000 issues Additionally, management will be proactive in sector outreach and will continue to implement the DoD Year 2000 Management Plan and its revisions and other DoD and Presidential guidance. See the finding for a summary of management comments and the Defense Technology Security Administration Comments section for the complete text of the comments

Table of Contents

Executive Summary i

Introduction

Background 1
Objectives 3

Finding

Status of the Defense Technology Security Administration Year 2000 Program 4

Appendixes

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

Management Comments

Defense Technology Security Administration 13

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 to 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 March 31, 1999, for non-mission-critical systems

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 the memorandum "Year 2000 Compliance" on August 7, 1998, and stated that the Y2K computer problem is a critical national Defense issue He also stated 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

Defense Technology Security Administration. The Defense Technology Security Administration (DTSA) was established in 1985 as a field activity of the Office of the Secretary of Defense By establishing DTSA, the DoD role in export controls was centralized and consolidated under the Under Secretary of Defense for Policy DTSA develops and implements DoD policy on international transfers of Defense-related goods, services, and technologies to ensure that such transfers are consistent with national security interests. The functions of DTSA include the following·

- managing the DoD license review process for dual-use and munitions licenses,
- developing technology security policies on the releasability of Defense-related systems and technologies to allies and friends,
- performing technical analyses and determining DoD positions on export control lists and associated regulations,
- participating in international export control negotiations on arms and sensitive dual-use goods and technology,
- providing technical support to U S efforts directed at the prevention of unauthorized technology transfers,
- determining DoD positions on the review of foreign investments in Defense-related companies, and
- providing technical support for other nations in the development of effective export control systems.

DTSA classified its systems as external and internal DTSA classified systems that it uses as remote systems but that were the responsibility of another organization as external Internal systems were those that DTSA owned and maintained. DTSA reported its mission-critical system as external, owned by the Office of the Under Secretary of Defense for Policy. DTSA also reported 17 non-mission-critical systems as external. DTSA reported 24 non-mission-critical systems as internal.

Defense Threat Reduction Agency. Under the auspices of the Defense Reform Initiative, DTSA merged with the On-Site Inspection Agency, the Defense Special Weapons Agency, 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.

Objectives

Our overall objective was to determine whether planning and management within DTSA were adequate to ensure that continuity of operations will not be unduly disrupted by Y2K-related issues. Specifically, the audit addressed the actions taken by DTSA to resolve date-processing issues regarding the year 2000, as well as preparation of plans to address Y2K-related system failures that could impact the ability of the Defense Threat Reduction Agency to perform its mission See Appendix A for a discussion of the audit scope and methodology and prior audit coverage.

Status of the Defense Technology Security Administration Year 2000 Program

The DTSA has recognized the importance of the Y2K issue and has taken positive actions to address the Y2K problem. However, further actions are necessary because DTSA did not complete all the actions that it should to minimize the potential adverse impact of Y2K date processing on its systems. Specifically, DTSA did not

- classify systems as Y2K compliant only after completing Y2K compliance checklists,
- submit quarterly reports to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence);
- develop written contingency plans, in accordance with the Draft DoD Management Plan, for any system the failure of which may cause disruptions to mission of DTSA;
- develop a continuity of operations plan to minimize Y2K disruption to the mission of DTSA, and
- take a proactive stance with regard to sector outreach

Unless the DTSA makes further progress on mitigating Y2K risks, DTSA, as 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 DTSA has taken the following actions as part of its effort to address the Y2K problem·

- appointing a Y2K point of contact,
- attending DoD Y2K interface assessment workshop meetings;
- including Y2K compliance language in new information technology contracts,
- beginning to address the Y2K issue in July 1996,
- contacting points of contact for external systems to determine Y2K compliance;
- contacting the point of contact for its mission-critical system to determine whether a contingency plan existed,

- testing personal computers for Y2K compliance and obtaining vendor certifications from the Internet to support Y2K compliance of hardware, operating systems, and commercial off-the-shelf software; and
- beginning the process of replacing or upgrading hardware, software, and operating systems that were not Y2K compliant

Compliance Certification

Certification Guidance. The Draft DoD Management Plan requires that the system developers or maintainers and the system's functional proponent certify and document each system's Y2K compliance. According to the Draft DoD Management Plan, certification of Y2K compliance for a system consists of a signature by the system manager, the project manager, and the customer on the checklist confirming the completion of testing in accordance with the Draft DoD Management Plan and confirming the results indicate that the system is compliant The signed checklist should be retained as part of the system documentation The signing of the Y2K compliance checklist holds individuals accountable for the determination of the Y2K compliance of a system. An example of a Y2K compliance checklist is in Appendix G of the Draft DoD Management Plan

Report on Certification. Inspector General, DoD, Report No 98-147, "Year 2000 Certification of Mission-Critical DoD Information Technology Systems," June 5, 1998, states that DoD Components are 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 have 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.

Certified Systems. DTSA did not complete Y2K compliance checklists for any systems that it owned and maintained. DTSA did not complete the checklists because it was not knowledgeable of the DoD Management Plan, and therefore, of the requirement for a Y2K compliance checklist. DTSA should not identify any of its systems as compliant until a Y2K compliance checklist is completed and signed. The purpose of the checklist is to assist system managers in ensuring that their systems are Y2K compliant.

Quarterly Reporting

DTSA did not report the status of its systems as required by the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) According to the Office of the Assistant Secretary of Defense

(Command, Control, Communications, and Intelligence), as of February 1998, DoD Components were required to report the status of non-mission-critical systems in their quarterly reports DTSA stated that it had contacted the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to determine whether it required DTSA to report the status of its systems and did not receive a response

Contingency Plans

The DTSA did not develop written contingency plans for its systems Contingency plans assist management in preparing for unanticipated system disruptions The Draft DoD Management Plan suggests developing contingency plans for any system the failure of which may cause disruptions to the functions of the DoD Component The Draft DoD Management Plan states that DoD Components should develop realistic contingency plans, including the development and activation of manual or contract procedures, to ensure the continuity of core processes DTSA stated that its mission could be executed by performing functions manually; however, procedures on manually performing its functions were not readily available In accordance with the Draft DoD Management Plan, DTSA should assess its systems to determine whether they need contingency plans and develop contingency plans for any system the failure of which may cause disruptions to the mission of DTSA

Continuity-of-Operations Plan

DTSA did not develop a continuity-of-operations plan to address its Y2K issues. The Draft DoD Management Plan states that DoD Components are responsible for developing a DoD Component continuity-of-operations plan The plan should include a prioritized list of systems and major actions taken to minimize Y2K disruptions In developing the continuity-of-operations plan, DTSA should review its whole environment, including the systems that DTSA uses but does not own and maintain For example, the Deputy Director of DTSA stated that the mission-critical system that DTSA used but did not own or maintain was essential for licensing. However, the point of contact from the Office of the Under Secretary of Defense for Policy for the mission-critical system did not respond to DTSA regarding whether a contingency plan exists for the system The lack of a continuity-of-operations plan may prevent DTSA from executing its part of the mission of the Defense Threat Reduction Agency

Sector Analysis

The President's Council on Year 2000 Conversion issued a draft "Sector Analysis for DoD Support" (sector analysis) dated June 11, 1998. The aim of the sector analysis is to have all actions of the Federal Government covered for Y2K 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 Two areas of interest that were assigned to DoD as the lead Federal agency were foreign military sales and nuclear weapons security and release procedures.

DTSA stated that it did not receive a direct tasking regarding the sector analysis. DTSA needs to keep informed of its role in the sector analysis and needs to be proactive in the area

DoD Management Plan

DTSA did not fully implement the DoD Management Plan and its revisions as guidance to deal with Y2K issues even though the DoD Management Plan applies to all DoD Components and all information technology systems DTSA personnel assigned to the Y2K issue were unaware of the DoD Management Plan. DTSA did not develop internal Y2K guidance but did issue a tasking requiring an inventory of all hardware and software The tasking also stated that copies of vendor Y2K compliance statements were to be maintained The tasking requested that the DTSA Y2K team research areas where companies did not provide a clear guarantee on their information technology The DoD Management Plan would have provided DTSA important guidance on the preparation of Y2K compliance checklists, quarterly reports, contingency plans, and a continuity-of-operations plan

Conclusion

Although DTSA made initial progress, DTSA must continue to address several critical issues The DTSA has recognized the importance of solving Y2K problems in systems to reduce the risk of Y2K failure, but DTSA must take a more aggressive approach in documenting Y2K compliance Therefore, DTSA must continually monitor and assess the progress of Y2K compliance and report the results in quarterly reports Additionally, DTSA needs to complete compliance checklists, contingency plans as appropriate, and a continuity-of-operation plan.

Recommendations and Management Comments

We recommend that the Director, Defense Technology Security Administration:

1. Report systems as compliant only after completing year 2000 compliance checklists.

2. Submit quarterly reports to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in accordance with the latest DoD quarterly report guidance.

3. Develop, as appropriate, written contingency plans, in accordance with the DoD Year 2000 Management Plan and its revisions, for any system the failure of which may cause disruptions to mission of the Defense Technology Security Administration.

4. Develop a continuity-of-operations plan, in accordance with the DoD Year 2000 Management Plan, For Signature Draft Version 2.0, to minimize year 2000 disruption to the mission of the Defense Technology Security Administration as a part of the mission of the Defense Threat Reduction Agency.

5. Assume a proactive stance with regard to sector outreach, both domestically and internationally, in areas relating to the mission of the Defense Technology Security Administration as a part of the Defense Threat Reduction Agency.

6. Implement the DoD Year 2000 Management Plan and its revisions and other DoD and Presidential Guidance.

Management Comments. The Director, Defense Technology Security Administration, concurred with the recommendations, stating that management has developed a compliance checklist and is currently testing components Management is also preparing quarterly reports Under the Defense Threat Reduction Agency, contingency plans will be developed by December 31, 1998, and the continuity-of-operations plan will be updated to address year 2000 issues by March 31, 1999 Additionally, management will be proactive in sector outreach and will continue to implement the DoD Year 2000 Management Plan and its revisions and other DoD and Presidential guidance

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 the issue, see the Y2K webpage on IGnet at http://www.ignet gov.

Scope

We reviewed and evaluated the status of the progress of DTSA in resolving the Y2K computing issue We evaluated the Y2K efforts of DTSA, 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 and the Draft DoD Management Plan issued in June 1998 We obtained documentation including the systems inventory status information as of August 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, the Department of Defense has established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting the objectives This report pertains to achievement of the following objective and goal

- **Objective:** Prepare now for an uncertain future
- **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. **(DoD-3)**

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

Summary of Prior Coverage

The General Accounting Office and 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, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, 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

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 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

Defense Technology Security Administration Comments

DEFENSE TECHNOLOGY SECURITY ADMINISTRATION
400 ARMY NAVY DRIVE, SUITE 300
ARLINGTON, VA 22202-2884

October 14, 1998
As of September 30, 1998

MEMORANDUM FOR DIRECTOR ACQUISITION MANAGEMENT, DEPARTMENT OF DEFENSE INSPECTOR GENERAL (DOD IG)

FROM: DIRECTOR, DEFENSE TECHNOLOGY SECURITY ADMINISTRATION
Prepared by: Carolyn Slavin, 604-5175

SUBJECT: Response to Draft DOD IG Audit Report on Year 2000 Program, Project No 8AS-0032.05, dated September 16, 1998

Thank you for the opportunity to review and comment on your September 16, 1998, draft audit report on reporting requirements for the Year 2000 (Y2K) information technology systems.

I am providing the attached comments on the behalf of the Defense Technology Security Administration (DTSA) Our comments reflect the state of our work in addressing the Y2K problem up to September 30, 1998. As you know DTSA, merged into the Defense Threat Reduction Agency (DTRA) on October 1, 1998, thus, work on the Y2K issues relevant to DTSA will be continued by DTRA.

Attachment:
DTSA Audit Response

Response of the Defense Technology Security Administration
to the Office of the Inspector General (IG)
DoD Draft Audit Report on
"Management of the Defense Technology Security Administration
Year 2000 Program"
Project No. 8AS-0032.05

The Defense Technology Security Administration (DTSA) has been actively addressing the "Year 2000" (Y2K) problem for over two years. DTSA's work was prompted by C3I's 8 May 1998 memorandum ("Year 2000 (Y2K) Computing Problem with Personal Computers and Workstations"). In its 8 August 1996 response to that memorandum DTSA stated that "To immediately enforce the Y2K compliance, DTSA requires 2000 standards on all procurement and development of new hardware, vendor software, data bases, in-house source code, electronic forms, etc." This guidance was enforced throughout DTSA from that point in time forward When the IG initiated its audit in September of 1998, DTSA believed it was in full compliance with the referenced guidance.

During the Y2K audit the IG brought to our attention more recent DoD guidance on Y2K that had not been distributed to the "Directors of the DOD Field Activities", nor received by DTSA through other channels. The guidance included: Secretary of Defense memorandum, dated 7 August 1998, concerning "Year 2000 Compliance"; Deputy Secretary Defense memorandum, dated 24 August 1998, concerning "Year 2000 (Y2K) Verification of National Security Capabilities"; draft "Sector Analysis for DoD Support for the President's Council on Year 2000 Conversion," dated 11 June 1998; and the June 1998 "Draft DoD Year 2000 Management Plan (version 2 0) " The chief difference between the procedures followed by DTSA and those requirements of more recent guidance concerns the checklist of procedures to track Y2K compliance Current guidance requires greater detail in documenting how compliance is verified and certification of compliance by certain officials IN addition, current guidance requires development of contingency plans for system failure As discussed more fully below, since the IG audit, DTSA has revised its checklist and taken other steps to comply with the new guidance

Responses to the specific **recommendations** in the referenced report are listed below:

Recommendation 1: The DoD/IG recommended that DTSA report systems as compliant only after completing year 2000 compliance checklists.

Response: Concur. DTSA has developed a compliant checklist based on Appendix G of the Draft DoD Year 2000 Management Plan (version 2.0) and is currently in the process of testing all hardware/software components used by DTSA. We are advised that the OMB target completion date for the validation

phase for all systems is January 31, 1999. All validation should be completed prior to this date

Recommendation 2: The DoD/IG recommended that DTSA submit quarterly reports to the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) in accordance with the latest DoD quarterly report guidance.

Response: Concur. In accordance with the guidance provided by the ASD(C3I) Year 2000 Oversight and Contingency Planning Office, DTSA began preparing the electronic file for quarterly reports Estimated date of completion is on or before October 23, 1998

Recommendation 3: The DoD/IG recommended that DTSA develop, as appropriate, written contingency plans, in accordance with the DoD Year 2000 Management Plan and its revisions, for any system the failure of which may cause disruptions to the mission of the Defense Technology Security Administration.

Response: Concur. In this correction, it should be noted that DTSA does not own mission critical systems. Contingency plans for failure of systems will be developed by DTRA. In accordance with the guidance provided by the DoD Y2K Oversight and Contingency Planning Office and the Draft DoD Year 2000 Management Plan (version 2.0) the deadline for contingency plans for mission critical systems is December 31, 1998, and for non-mission critical as soon as possible DTSA estimates that written contingency plans will be completed by these timelines

Recommendation 4: The DoD/IG recommended that DTSA develop a continuity-of-operation plan, in accordance with the DoD Year 2000 Management Plan, For Signature Draft Version 2 0, to minimize year 2000 disruption to the mission of the Defense Technology Security Administration as a part of the mission of the Defense Threat Reduction Agency

Response: Concur. DTSA's Automated Information System Security Plan (AISSP) has a continuity of operation plan, but does not address the Y2K issue. This will be updated by DTRA The DoD Y2K Oversight and Contingency Planning Office and the Draft DoD Year 2000 Management Plan (version 2 0), stated the target completion date for the continuity-of-operation plan is March 31, 1999 DTSA estimates the continuity-of-operation plan will be completed on or before this date

Recommendation 5: The DoD/IG recommended that DTSA assume a proactive stance with regard to sector outreach, both domestically and internationally, in areas relating to the mission of the Defense Technology Security Administration as a part of the Defense Threat Reduction Agency.

Response: Concur. DTSA determined that the Defense/International Security Sector is relevant to DTSA's mission A DTRA representative will be selected to participate in that sector outreach program by October 23, 1998

Recommendation 6: The DoD/IG recommended that DTSA implement the DoD Year 2000 Management Plan and its revisions and other DoD and Presidential Guidance.

Response: Concur DTSA has participated in the DoD Year 2000 Working Group. Also, as indicated above, DTSA established an effective Y2K process that made significant progress toward achieving the objectives of the DoD Year 2000 Management Plan, its revisions and all other DoD and Presidential Guidance Work will be continued by DTRA.

The DTSA POC for Y2K is Carolyn Slavin (604-5175).
The DTRA POC for Y2K is Capt. Allan Toole (325-6332)

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
Deborah L Carros
Virginia G Rogers
Jennifer L. Zucal

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Management of the Defense Technology Security Administration Year 2000 Program

B. DATE Report Downloaded From the Internet: 09/07/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 09/07/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.