Audit Report

MANAGEMENT OF THE DEFENSE SPECIAL WEAPONS AGENCY YEAR 2000 PROGRAM

Report No. 99-028

October 30, 1998

Office of the Inspector General
Department of Defense

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

DSWA	Defense Special Weapons Agency
Y2K	Year 2000

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

October 30, 1998

MEMORANDUM FOR DIRECTOR, DEFENSE THREAT REDUCTION AGENCY

SUBJECT: Audit Report on Management of the Defense Special Weapons Agency Year 2000 Program (Report No. 99-028)

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 Special Weapons Agency concurred with the recommendations.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Virginia G. Rogers at (703) 604-9041 (DSN 664-9041) (vrogers@dodig.osd.mil), Ms. Kathryn M. Truex at (703) 604-9045 (DSN 664-9045) (kmtruex@dodig.osd.mil), or Ms. Mary Lu Ugone at (703) 604-9049 (DSN 664-9049) (mlugone@dodig.osd.mil). See Appendix B for the report distribution. The audit team members are listed inside the back cover.

Robert J Lieberman

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-028 **October 30, 1998**
(Project No. 8AS-0019)

Management of the Defense Special Weapons Agency 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 the Defense Special Weapons Agency was adequately preparing its information technology systems to resolve date-processing issues regarding the year 2000. Specifically, the audit evaluated whether the Defense Special Weapons Agency complied with the DoD Year 2000 Management Plan.

Results. The Defense Special Weapons 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 Defense Special Weapons Agency made in resolving the year 2000 computing issue is not complete. Unless the Defense Special Weapons Agency makes further progress on mitigating year 2000 risks, the Defense Special Weapons Agency, 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 Special Weapons Agency, report systems as compliant only after completing year 2000 testing and year 2000 compliance checklists, develop contingency plans for its mission-critical systems and any other system the failure of which may cause disruptions to the Defense Special Weapons Agency's mission, update the continuity-of-operations plan to specifically address the year 2000 issue, assume a proactive stance with regard to sector outreach, and implement revisions to the DoD Year 2000 Management Plan and other DoD and Presidential guidance.

Management Comments. The Director, Defense Special Weapons Agency, concurred with the draft recommendations, stating that management will review all systems currently reported as compliant and change the status of systems for which proper documentation does not exist. Management will also develop contingency plans for all mission-critical systems and will update its continuity-of-operations plan to address year 2000 issues. Finally, management will be proactive in regard to sector outreach and will implement the core ideas from the revisions to the DoD Year 2000 Management Plan that have survived at least one revision. See the finding for a summary of management comments and the Defense Special Weapons Agency Comments section for the complete text of the comments.

Table of Contents

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 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 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 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 Special Weapons Agency. The Armed Forces Special Weapons Project was created in 1947 to conduct nuclear weapon effects research and provide nuclear technical, logistical, and training support for DoD. Renamed the Defense Atomic Support Agency in 1959 and the Defense Nuclear Agency in 1971, the Agency became the Defense Special Weapons Agency (DSWA) in 1996 as the result of a new charter and an expanded mission.

DSWA is the center for nuclear and advanced weapons effects expertise for the DoD. The mission of DSWA is to research and develop technologies to support military systems and satisfy operational requirements. To accomplish its mission, DSWA:

- manages the military nuclear weapons stockpile support and conducts programs associated with the Cooperative Threat Reduction, force protection, arms control technology, and counterproliferation support;
- provides emergency response support and planning assistance for nuclear weapons accidents or improvised nuclear device incidents;
- maintains the scientific expertise and develops data necessary to ensure advanced conventional systems, nuclear systems, and command and control assets will continue to operate in potential nuclear environments; and
- supports U.S. Government implementation, compliance, and verification of arms control treaties and agreements.

Defense Threat Reduction Agency. Under the auspices of the Defense Reform Initiative, DSWA merged with the On-Site Inspection Agency, the Defense Technology Security Agency, and some program functions of the Assistant to the Secretary of Defense for the 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 matters of weapons of mass destruction to DoD Components.

Objectives

Our overall objective was to determine whether DSWA was adequately preparing its information technology systems to resolve date-processing issues regarding Y2K. Specifically, the audit evaluated whether DSWA had complied with the DoD Year 2000 Management Plan. See Appendix A for a discussion of the audit scope and methodology and prior audit coverage.

Status of the Defense Special Weapons Agency Year 2000 Program

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

- classify systems as Y2K compliant only after completing independent testing of the systems and Y2K compliance checklists and document the process for testing its systems,
- develop written contingency plans for mission-critical systems and any other system for which failure may cause disruptions to the mission of DSWA,
- update the continuity-of-operations plan, in accordance with the Draft DoD Management Plan, to minimize Y2K disruptions to the mission of DSWA as a part of the Defense Threat Reduction Agency, and
- take a proactive stance with regard to sector outreach in areas for the mission of DSWA as a part of the Defense Threat Reduction Agency.

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

- appointed a Y2K point of contact,
- adopted the April 1997 DoD Management Plan,
- included Y2K compliance language in all new information technology contracts,
- attended DoD Y2K interface assessment workshops and Y2K working group meetings, and
- began the process of replacing or upgrading hardware, software, and operating systems that are not Y2K compliant.

Testing and Compliance Certification

Testing. DSWA did not complete independent testing of three mission-critical systems before classifying them as Y2K compliant. According to the Draft DoD Management Plan, the Office of Management and Budget requires independent verification of systems reported as Y2K compliant. The Draft DoD Management Plan states that DoD Components need an extensive period of time to adequately validate and test converted or replaced systems for Y2K compliance. Renovated systems must be tested for any new software bugs introduced while fixing Y2K problems. 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.

The Draft DoD Management Plan strongly 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 homepage as being Y2K compliant. DSWA should document the basis for determining Y2K compliance of its commercial off-the-shelf products.

Testing Mission-Critical Systems. DSWA classified one mission-critical system, the Nuclear Management Information System, as compliant after testing was completed; however, three other mission-critical systems were classified as compliant prior to testing the systems. DSWA has since tested two of the three systems. DSWA tested the Nuclear Weapons Contingency Operations Module and the Nuclear Inventory Management Accounting Control System August 28, 1998. DSWA is currently reviewing the code for the Nuclear Inventory Management Accounting Control System and will begin testing the new version of the Special Weapons Information Management System at the end of September.

Testing Non-Mission-Critical Systems. DSWA provided documentation to support testing for 2 of the 10 non-mission-critical systems classified as compliant. For the remaining systems, 1 system does not use date calculations and 7 systems require vendor certifications.

DSWA has not documented a process for testing its mission-critical systems and non-mission-critical systems. Documenting a testing process would provide guidance for personnel required to test systems and would ensure that personnel test all pertinent aspects of Y2K issues for each system.

Compliance Certification. 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 results indicating that the system is compliant. DSWA 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 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 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.

Certifying Mission-Critical Systems. DSWA classified three of its mission-critical systems, the Special Weapons Information Management System, the Nuclear Weapons Contingency Operations Module, and the Nuclear Inventory Management Accounting Control System, as compliant but had not provided a compliance checklist as of September 4, 1998, confirming the completion of testing. DSWA determined that the Special Weapons Information Management System was Y2K compliant through vendor certifications, but is in the process of replacing the system with a newer version. The Nuclear Weapons Contingency Operations Module is currently under development. DSWA identified and fixed some date problems with the Nuclear Inventory Management Accounting Control System. DSWA provided a Y2K compliance checklist signed June 30, 1998, for the mission-critical system the Nuclear Management Information System.

Certifying Non-Mission-Critical Systems. DSWA provided signed checklists for 2 of the 10 non-mission-critical systems classified as compliant or complete. DSWA should not identify any of its systems as compliant before completing and signing a Y2K compliance checklist. The purpose of the checklist is to assist system managers in ensuring that their systems are Y2K compliant.

System Reclassification. The Quarterly Report that DSWA prepared on July 30, 1998, for the Office of the Secretary of Defense provides the Y2K status as of July 15, 1998, for systems owned by DSWA. The Y2K status of systems as reported in the Quarterly Report differs from the status of systems as reported in a systems inventory received on July 8, 1998, because the Quarterly Report reflects a more thorough review of the Y2K status of the systems that DSWA owned.

Contingency Plans

The DSWA had not developed written contingency plans for its five mission-critical systems. Contingency plans assist management in preparing for unanticipated system disruptions. The DoD Management Plan recommends developing contingency plans and the Draft DoD Management Plan suggests developing contingency plans for any systems of which the failure may cause disruptions to the functions of the component. The 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. In accordance with the Draft DoD Management Plan, DSWA should assess its mission-critical 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 DSWA.

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 disruptions. DSWA had a continuity-of-operations plan, but the plan did not address Y2K issues. Because DSWA became part of the Defense Threat Reduction Agency on October 1, 1998, DSWA needs to address its Y2K issues as they relate to 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. Areas of interest that the Sector Analysis assigned to DoD as the lead Federal agency included:

- Defense treaties and alliances,
- Defense treaty obligations, and
- areas such as nuclear weapons security and release procedures.

DSWA stated that the areas in the Sector Analysis did not apply to the mission of DSWA and that DSWA had not received a direct tasking regarding the Sector Analysis. DSWA needs to keep informed in its role in the Sector Analysis and be proactive in the area.

Conclusion

Although DSWA made initial progress, DSWA must continue to address several critical issues. The DSWA has recognized the importance of solving Y2K problems in systems to reduce the risk of Y2K failure, but DSWA must take a more aggressive approach in documenting and testing for Y2K compliance. Therefore, DSWA must continually monitor and assess the progress of Y2K compliance, complete Y2K compliance checklists and contingency plans, and document system testing. DSWA also needs to be diligent about staying current in implementing revisions to the DoD Year 2000 Management Plan and other DoD and Presidential guidance.

Recommendations and Management Comments

We recommend that the Director, Defense Special Weapons Agency:

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

2. Develop contingency plans in accordance with the DoD Year 2000 Management Plan and its revisions for its mission-critical systems and, if appropriate, any system of which its failure may cause disruptions to the Defense Special Weapons Agency's mission.

3. Update the continuity-of-operations plan to specifically address the year 2000 issue and Defense Special Weapons Agency's mission as it relates to the mission of the Defense Threat Reduction Agency.

4. Assume a proactive stance with regard to sector outreach, both domestically and internationally, in areas relating to the Defense Threat Reduction Agency's mission.

5. Stay current in implementing revisions to the DoD Year 2000 Management Plan and other DoD and Presidential guidance.

Management Comments. The Director, Defense Special Weapons Agency concurred with the draft recommendations. Management will review all systems currently reported as compliant and change the status of systems for which proper documentation does not exist. Management will also develop contingency plans for all mission-critical systems and will update its continuity-of-operations plan to address year 2000 issues. Additionally, management will be proactive in regard to sector outreach and will implement the core ideas from the revisions to the DoD Year 2000 Management Plan that have survived at least one revision.

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 DSWA in resolving the Y2K computing issue. We evaluated the Y2K efforts of DSWA, 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 July 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 objectives and goals.

- **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 September 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.

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

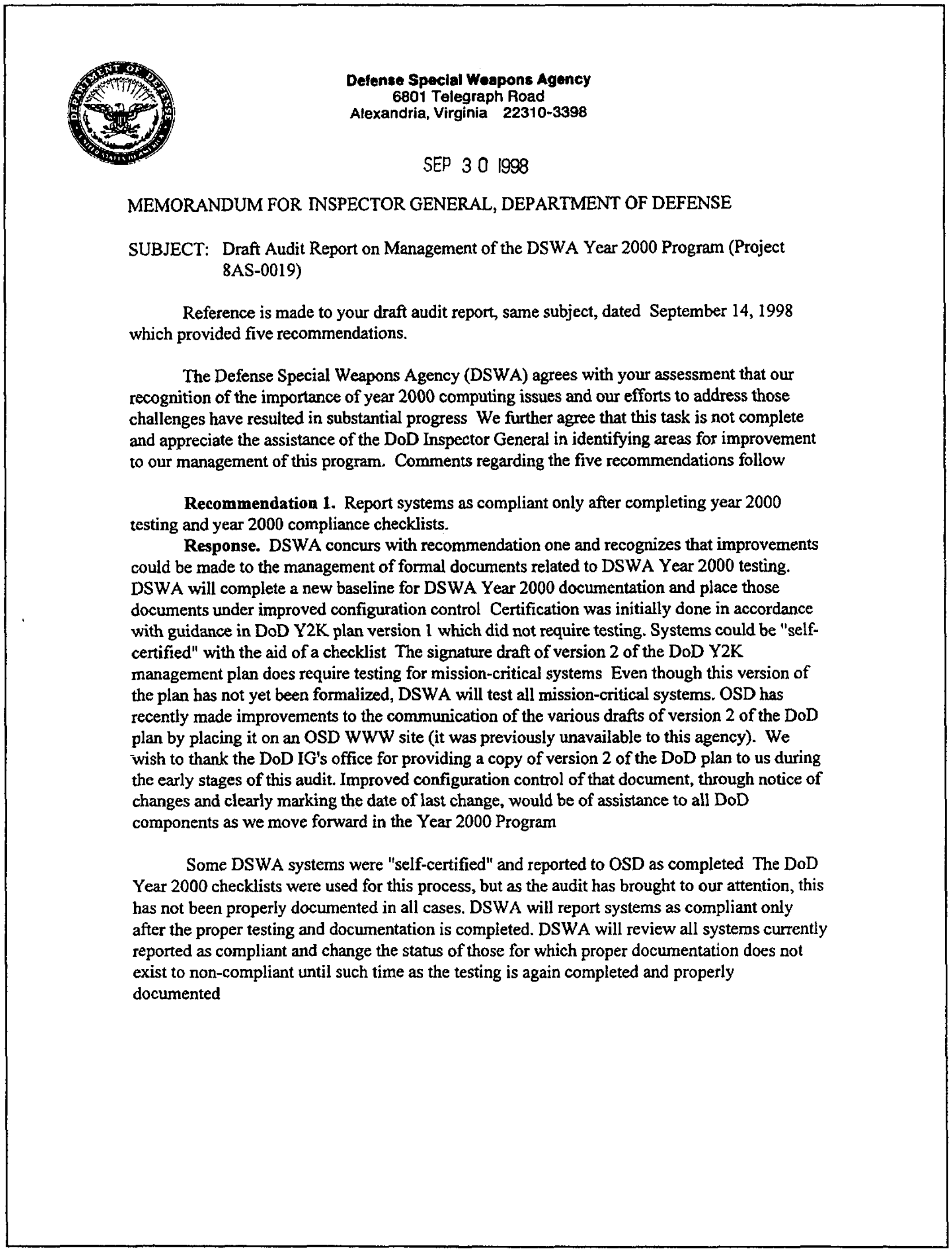
Non-Defense Federal Organizations and Individuals

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 Special Weapons Agency Comments



Defense Special Weapons Agency
6801 Telegraph Road
Alexandria, Virginia 22310-3398

SEP 3 0 1998

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Draft Audit Report on Management of the DSWA Year 2000 Program (Project 8AS-0019)

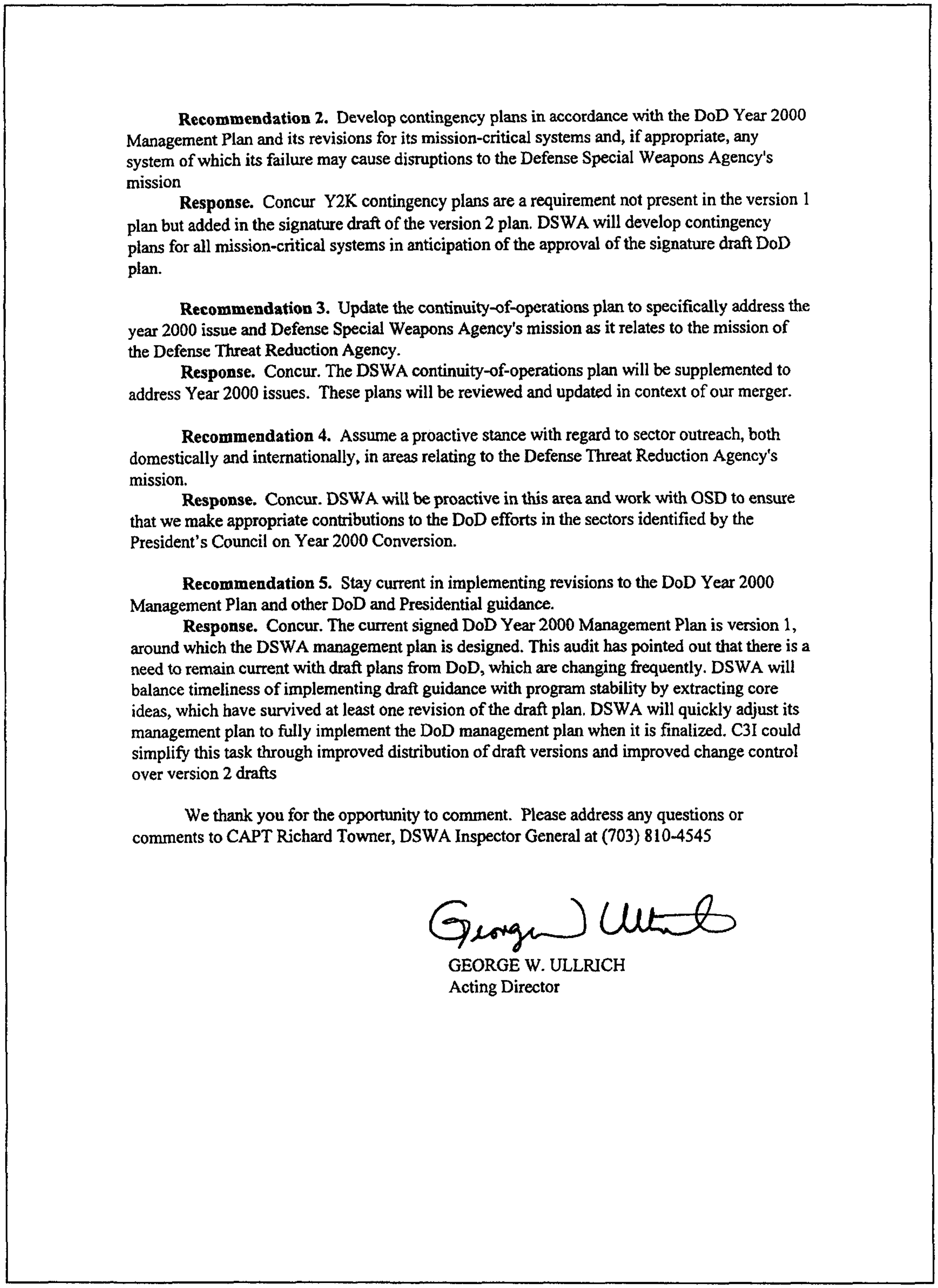
Reference is made to your draft audit report, same subject, dated September 14, 1998 which provided five recommendations.

The Defense Special Weapons Agency (DSWA) agrees with your assessment that our recognition of the importance of year 2000 computing issues and our efforts to address those challenges have resulted in substantial progress We further agree that this task is not complete and appreciate the assistance of the DoD Inspector General in identifying areas for improvement to our management of this program. Comments regarding the five recommendations follow

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

Response. DSWA concurs with recommendation one and recognizes that improvements could be made to the management of formal documents related to DSWA Year 2000 testing. DSWA will complete a new baseline for DSWA Year 2000 documentation and place those documents under improved configuration control Certification was initially done in accordance with guidance in DoD Y2K plan version 1 which did not require testing. Systems could be "self-certified" with the aid of a checklist The signature draft of version 2 of the DoD Y2K management plan does require testing for mission-critical systems Even though this version of the plan has not yet been formalized, DSWA will test all mission-critical systems. OSD has recently made improvements to the communication of the various drafts of version 2 of the DoD plan by placing it on an OSD WWW site (it was previously unavailable to this agency). We wish to thank the DoD IG's office for providing a copy of version 2 of the DoD plan to us during the early stages of this audit. Improved configuration control of that document, through notice of changes and clearly marking the date of last change, would be of assistance to all DoD components as we move forward in the Year 2000 Program

Some DSWA systems were "self-certified" and reported to OSD as completed The DoD Year 2000 checklists were used for this process, but as the audit has brought to our attention, this has not been properly documented in all cases. DSWA will report systems as compliant only after the proper testing and documentation is completed. DSWA will review all systems currently reported as compliant and change the status of those for which proper documentation does not exist to non-compliant until such time as the testing is again completed and properly documented



Recommendation 2. Develop contingency plans in accordance with the DoD Year 2000 Management Plan and its revisions for its mission-critical systems and, if appropriate, any system of which its failure may cause disruptions to the Defense Special Weapons Agency's mission

Response. Concur Y2K contingency plans are a requirement not present in the version 1 plan but added in the signature draft of the version 2 plan. DSWA will develop contingency plans for all mission-critical systems in anticipation of the approval of the signature draft DoD plan.

Recommendation 3. Update the continuity-of-operations plan to specifically address the year 2000 issue and Defense Special Weapons Agency's mission as it relates to the mission of the Defense Threat Reduction Agency.

Response. Concur. The DSWA continuity-of-operations plan will be supplemented to address Year 2000 issues. These plans will be reviewed and updated in context of our merger.

Recommendation 4. Assume a proactive stance with regard to sector outreach, both domestically and internationally, in areas relating to the Defense Threat Reduction Agency's mission.

Response. Concur. DSWA will be proactive in this area and work with OSD to ensure that we make appropriate contributions to the DoD efforts in the sectors identified by the President's Council on Year 2000 Conversion.

Recommendation 5. Stay current in implementing revisions to the DoD Year 2000 Management Plan and other DoD and Presidential guidance.

Response. Concur. The current signed DoD Year 2000 Management Plan is version 1, around which the DSWA management plan is designed. This audit has pointed out that there is a need to remain current with draft plans from DoD, which are changing frequently. DSWA will balance timeliness of implementing draft guidance with program stability by extracting core ideas, which have survived at least one revision of the draft plan. DSWA will quickly adjust its management plan to fully implement the DoD management plan when it is finalized. C3I could simplify this task through improved distribution of draft versions and improved change control over version 2 drafts

We thank you for the opportunity to comment. Please address any questions or comments to CAPT Richard Towner, DSWA Inspector General at (703) 810-4545

George Ullrich

GEORGE W. ULLRICH
Acting Director

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
Michael T. Carlson