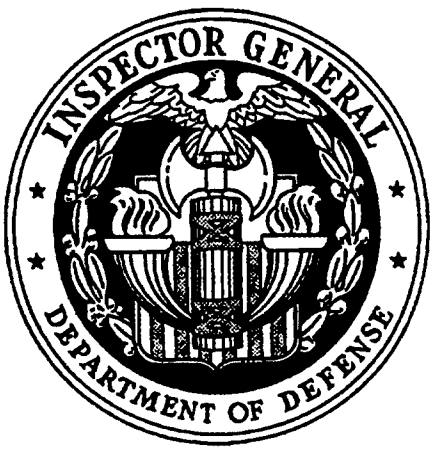
Audit Report



MANAGEMENT OF THE DEFENSE INFORMATION SYSTEMS AGENCY YEAR 2000 PROGRAM

Report No. 98-184 August 4, 1998

Office of the Inspector General
Department of Defense

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

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, Virginia 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

ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
DISA	Defense Information Systems Agency
Y2K	Year 2000

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

August 4, 1998

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Audit on Management of the Defense Information Systems Agency Year 2000 Program (Report No. 98-184)

We are providing this audit report for review and comment. We considered comments on the draft report in preparing the final report.

Comments on the draft report generally conformed to the requirements of DoD Directive 7650.3. However, DISA needs to clarify with DoD officials whether system interface agreements have to be formally established for selected communications systems. DoD Directive 7650.3 requires that all recommendations be resolved promptly and there is special urgency regarding Year 2000 conversion issues. Accordingly, we ask that you provide planned actions and completion dates regarding this issue by September 4, 1998.

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) or Mr. James W. Hutchinson at (703) 604-9060 (DSN 664-9060). See Appendix C for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-184 **August 4, 1998**
(Project No. 8AS-0005)

Management of the Defense Information Systems Agency Year 2000 Program

Executive Summary

Introduction. This report is one of a series being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge.

The cause of the year 2000 problem is that automated systems typically use two digits to represent the year, such as "98" representing 1998, to conserve on electronic data storage and reduce operating costs. With this two-digit format, however, the year 2000 is indistinguishable from 1900, or 2001 from 1901. As a result of the ambiguity, system or application programs that use dates to perform calculations, comparisons, or sorting could generate incorrect results when working with years after 1999. Unless the problem is corrected, the automated systems may fail. Therefore, DoD management issued a Year 2000 Management Plan that provides an overall strategy to assist the DoD Components in resolving problems related to the year 2000. The five phases included in the strategy are awareness, assessment, renovation, validation, and implementation.

Audit Objectives. The audit objective was to evaluate the Defense Information Systems Agency progress in preparing its information and technology systems for year 2000 compliance. This report discusses the program management of the year 2000 initiatives.

Audit Results. The Defense Information Systems Agency had implemented numerous actions to improve its year 2000 program, but some changes are still needed. We briefed management regarding the limited documentation available to support the year 2000 work progress specifically related to the dissemination of guidance, prioritizing interface identification, funding, contingency planning, testing and certification. Without a greater effort by the Defense Information Systems Agency to revise its year 2000 program to better comply with Federal and DoD requirements, the Defense Information Systems Agency faces increased risks that its information and technology systems may not operate properly in the year 2000 and beyond. The audit results are detailed in Part I.

Summary of Recommendations. We recommend that the Director, Defense Information Systems Agency, update the management plan to incorporate the changes to the extent of the guidance documented within the DoD Year 2000 Management Plan; disseminate guidance to the operating level; follow the exit criteria prescribed in the DoD Year 2000 Management Plan to accurately document the reported progress for year 2000; identify all interfaces to resolve any problems and communicate the resolutions to all interface partners; provide cost estimates for each system; develop

contingency plans for systems that will not complete the revised implementation phase scheduled for December 1998; and determine system year-2000 compliance status only after the system has been tested and certified as compliant.

Management Comments. DISA generally concurred with the recommendations and described both ongoing and newly initiated actions to improve DISA internal Y2K guidance and requirements and to ensure that it includes DoD-wide Y2K requirements related to system interface agreements, tracking Y2K costs, and formally certifying that DISA systems are Y2K compliant. DISA also commented that the status of DISA systems presented in the report is outdated and does not accurately reflect the current status of DISA systems. They also described extensive efforts to ensure that Y2K guidance, requirements, and other related information, reaches those who are directly involved in Y2K efforts. See Part 1 for a summary of management comments and Part III for the complete text of the comments.

Audit Response. DISA comments were generally responsive. We recognize that DISA has made commendable improvements in its Y2K efforts since we began the audit. Especially noteworthy are DISA efforts to disseminate Y2K requirements and information down to "the trenches." However, in verifying DISA actions taken on the recommendations, we could not confirm that DoD Y2K officials had waived interface agreement requirements for telecommunications transport systems. DISA believes that a need for interface agreements is obviated through adherence to international and national standards and that DoD had provided an exemption in that regard. We were unable to verify such an exemption in the DoD Y2K Management Plan or within the Office of Year 2000 Oversight and Contingency Planning. We ask that DISA clarify the DoD requirement for Y2K system interfaces for communications transport systems with DoD Y2K officials and provide comments on this final report by September 4, 1998. The response should specify what actions have been agreed to with the Office of Year 2000 Oversight and Planning and estimated completion dates.

Table of Contents

Part I - Audit Results

Audit Background

The cause of the year 2000 (Y2K) problem is that automated systems typically use two digits to represent the year, such as "98" representing 1998, to conserve on electronic data storage and reduce operating costs. With this two-digit format, however, the Y2K is indistinguishable from 1900, or 2001 from 1901. As a result of the ambiguity, system or application programs that use dates to perform calculations, comparisons, or sorting could generate incorrect results when working with years after 1999. Calculation of Y2K dates is further complicated because the year 2000 is a leap year, the first century leap year since 1600. This means that computer systems and applications must recognize February 29, 2000, as a valid date. Unless the problem is corrected, the automated systems may fail.

Because of the potential failure of computers to run or function throughout the Government, the President issued an executive order, "Year 2000 Conversion," dated February 4, 1998, making it policy that Federal agencies ensure that no critical Federal program is disrupted because of the Y2K problem. In addition, the head of each agency must ensure that efforts to address the Y2K problem receive the highest priority attention in the agency. Further, the General Accounting Office has designated resolution of the Y2K problem as a high-risk area, and DoD has recognized the Y2K issue as a material management control weakness area in the FY 1997 Annual Statement of Assurance.

Impact on DoD. As of January 1998, DoD reported 2,915 mission-critical systems*. Of those systems, 530 were Y2K compliant, 330 were scheduled to be replaced, 1,891 were being repaired, and 164 were being retired. The total cost of the DoD Y2K effort is estimated at about $2 billion.

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 includes a description of the five-phase Y2K management process. The most current DoD Management Plan, For Signature Draft Version 2.0, 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.

*A system that when its capabilities are degraded, the organization realizes a resulting loss of a core capability.

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

Defense Information Systems Agency. The Defense Information Systems Agency (DISA) is the DoD agency responsible for information technology and is the central manager for major portions of the DoD information infrastructure. As a result, DISA is obligated to provide Y2K-compliant computing platforms, networks, and services to the Services, DoD Components, and other customers.

Separate Y2K coordination responsibilities are assigned for the DISA-owned DoD corporate systems and the internal DISA-owned systems. The Office of the Deputy Director for Command, Control, Communications, Computers, and Intelligence has responsibility for the DISA-owned corporate systems, and the Office of the Chief Information Officer manages the internal DISA-owned systems. For oversight and coordination purposes, the Vice Director meets weekly with representatives of each DISA Directorate to discuss progress made and to help resolve problems related to the DISA Y2K program.

Audit Objective

The objective of the audit was to determine whether DISA is adequately preparing its information technology systems to resolve the date-processing issues for Y2K. Specifically, the objective was to determine whether the DISA has complied with the DoD Management Plan.

Status of the Defense Information Systems Agency Year 2000 Program

The DISA has recognized the importance of Y2K and has taken numerous positive actions in addressing the Y2K problem. However, DISA needs to address the following critical factors to be in compliance with the DoD Management Plan:

- update the DISA Y2K Problem Management Plan (hereafter referred to as the DISA Y2K Management Plan), dated November 20, 1996, to include the requirements of the DoD Management Plan;

- disseminate the DoD Management Plan, the DISA Y2K Management Plan, and other guidance in entirety to the operating levels;

- accurately report and document DISA Y2K status as prescribed in the exit criteria within the DoD Management Plan;

- identify all interfaces and assigning risk and efforts to resolve Y2K problems for document agreements with interface partners on how the interfaces should be made Y2K compliant;

- prepare updated Y2K cost estimates for each system to determine whether additional funding is needed;

- develop contingency plans for mission-critical systems in accordance with the DoD Management Plan and communicating the plans to interface partners; and

- validate systems as Y2K compliant only after fully documenting test results using the official compliance checklists.

Unless DISA adequately addresses these issues, its mission-critical systems may not successfully operate in the year 2000 and beyond.

Actions Taken to Address the Year 2000 Problem

Recognizing the importance of Y2K, DISA implemented various positive actions to resolve the Y2K problem. For example, DISA established a Y2K program management structure to improve management awareness and to provide frequent high-level guidance and direction in developing and executing the DISA Y2K strategy.

The DISA efforts to address the Y2K problem include the following additional actions:

- DISA sponsored periodic meetings between systems' owners and the central design activities responsible for modifying the programs run by management representatives;

- DISA established DISA Y2K coordinators for DISA-owned DoD corporate systems and another for internal DISA-owned systems;

- DISA developed its Y2K Management Plan, which provides guidance on the strategies, policies, and procedures needed to identify and resolve Y2K issues;

- DISA rated the criticality of all its information systems and used the rating to categorize the systems as mission critical or non-mission critical;

- DISA identified sufficient funds to pay for all of its necessary Y2K solutions without affecting other necessary operations; and

- DISA developed the DISA Y2K Testing Guideline, dated December 30, 1997.

Also, the DISA Director required that all DISA-owned and maintained systems complete the Y2K implementation phase by October 1, 1998. The requirement accelerated the Y2K program milestones in the DoD Management Plan by 3 months for mission-critical systems and by 6 months for non-mission-critical systems. The major benefit of the requirement is that DISA will have a year to run its systems in an operational mode and to work out any problems before the turn of the century.

These aggressive actions by DISA are commendable. However, DISA needs to emphasize several Y2K issues more forcefully, as detailed in the following discussion. See Appendix B for a summary of issues related to the specific systems reviewed.

DISA Year 2000 Guidance

The DISA Y2K program coordinators need to devote greater efforts to updating the DISA Y2K Management Plan and disseminating current guidance to program and management representatives. A detailed summary of the results of the review is in Appendix B of this report.

Updating the DISA Y2K Management Plan. DISA needs to update its Y2K Management Plan and modify its strategy to more closely conform with the current version of the DoD Management Plan. The ASD(C^3I) signed Version 1.0 of the DoD Management Plan in April 1997. Later, the ASD(C3I) produced two updated versions and issued the unofficial Version 2.0 in January 1998.

DISA prepared the DISA Y2K Management Plan in November 1996, 6 months before the ASD(C3I) issued Version 1.0 of the DoD Management Plan. Because the DISA Y2K Management Plan preceded the DoD Management Plan, a management representative from the DISA Y2K Program Office stated that no plans would be made to modify the DISA Y2K Management Plan. The DISA Y2K Management Plan includes more restrictive time requirements than the most recent Version 2.0 of the DoD Management Plan; however, it is significantly more lenient in other areas, which is reflected in the results of this audit. The DISA Y2K Management Plan does not mirror the requirements of the DoD Management Plan for contingency planning, estimating Y2K costs, identifying time and other resource requirements, procurement planning, or preparing written Y2K strategies.

Dissemination of Guidance. DISA not only needs to update its DISA Y2K Management Plan but also needs to make its component organizations more fully aware that DISA and DoD have published useful Y2K strategies and requirements. We spoke with 24 manager representatives responsible for the 35 separate systems in our sample. Of the 24 management representatives, 14 were not knowledgeable of the DoD Management Plan or the DISA Y2K Management Plan. However, the lack of awareness should not prevent the management representatives from taking specific actions to resolve any Y2K issues. We encourage DISA to disseminate both documents because they are useful and necessary resources for system and program managers working the Y2K issues. The DoD Management Plan outlines responsibilities and milestones and provides guidelines to ensure that no system fails because of Y2K problems.

The DoD Management Plan provides DISA component organizations with specific requirements for the five-phase management process and with exit criteria for reporting the progression from one phase to the next. Furthermore, DISA already has instructed management representatives to report the Y2K progression status in accordance with the requirements of the DoD Management Plan. The review identified that DISA management had not adequately documented the Y2K progression status.

Documentation

We met or consulted with system managers responsible for DISA mission-critical information systems from November 1997 through February 1998. We looked for minimal information on problem definition, milestones for completion of each phase, resource requirements, procurement plans or other methods of making the system Y2K compliant, and asked DISA management representatives to provide written strategies for making their individual systems Y2K compliant. The DoD Management Plan requires that DoD Components and management representatives develop strategies to resolve their Y2K problems in passing from the assessment phase to the renovation phase. In our sample of 35 DISA information systems, with the exception of the 3 retired systems, the 3 systems already replaced or scheduled to be replaced, and the 2 systems managed but not owned by DISA, DISA reported 27 systems as either in the renovation phase or beyond. Of the 27 systems, 21 systems had no written Y2K strategy. However, the management representatives provided an acquisition strategy document dated December 24, 1997, that required all new information and technology items to be Y2K compliant. But, the DoD Management Plan requires a planned strategy to be completed in the assessment phase that shows the start and ending date of each phase, establishes major steps to convert and test Y2K solutions, and identifies the infrastructure and resources needed to complete the Y2K compliance. Also, the DoD Management Plan requires that the strategy be updated as exit criteria in each phase of the management process. Had the DISA management completed the required exit criteria, the interface identifications would have been completed, prioritized, documented, and available to assist the interface partners in readying their systems to meet the Y2K computer challenge.

Interface Identification Priority

The DoD Management Plan considers identification of interfaces to be the highest priority because the transfer of electronic data has the potential to introduce errors, propagate errors, or both from one DoD Component to another. As a result, the DISA management representatives should give greater priority to identifying interfaces, preparing written agreements with interface partners, and identifying Y2K solutions for the interfaces.

Interface Defined. The DoD Management Plan defines an interface as a boundary across which two systems pass electronic data. An interface might be a hardware connector or it might be a convention to allow communication between two software systems. Interfaces may connect applications, programs, or systems internally within DISA or between DISA and other DoD Components. Interfaces may also connect systems among DoD and external organizations.

Interface Identification. DISA has not completed the interface identification process. In the DISA report on Y2K status for the quarter ending January 1998, DISA identified 98 DISA-managed systems as mission critical and 127

DISA-managed systems as noncritical. Also, DISA reported a total of 225 interfaces for the mission-critical and non-mission-critical systems. A management representative from the Office of the Chief Information Officer stated that most DISA mission-critical systems do not interface with other internal or external systems, although many DISA systems interface with 20 or more systems. Of the 24 management representative we spoke with, 5 indicated that their systems did interface with others and readily stated that they had not yet started to identify interfaces.

Prioritization and Risk Assessment. The DoD Management Plan asks Components to identify all system interfaces and to use the assessment to prioritize mission-critical system interfaces for DISA and other organizations. Because DISA has not emphasized interface identification, it has not been able to prioritize the importance of the system for system interface partners. Recently, management representatives started to identify all interfaces, but the action is still ongoing. In one instance, a management representative provided updated information that showed one system's number of interfaces had increased to 96 since the initial review.

Documented Interface Agreements. After DISA identifies its interfaces, it needs to communicate when and in what manner it plans to resolve the specific interface issue, so that the partners will be able to accommodate DISA Y2K changes. The DoD Management Plan requires DoD Components to document and obtain system interface agreements in the form of a Memorandum of Agreement or its equivalent. A sample Y2K compliance checklist included in the DoD Management Plan states that DoD Components and each interface partner should negotiate an agreement dealing with Y2K issues. Also, each interface partner should discuss and verify consistent implementation of Y2K corrections for compliance when date data pass between systems.

Of the 25 systems in our sample for which interfaces were an issue, only one management representative had initiated a written interface agreement to support system interfaces that had been identified. From our sampled systems, DISA management stated that 13 systems did not need formal interface agreements because they are telecommunications transport systems and adhere to international standards. As such, DISA management stated that effecting interface agreements for telecommunications transport systems would be unnecessarily time-consuming and bureaucratic because they are not impacted by date actions tied to Y2K. We agree that formal interface agreements for telecommunications systems may not be appropriate, but also recognize that DoD guidance does not provide an exception for telecommunications systems. DoD may be willing to make that exception if DISA was better able to identify the costs involved.

Funding

To ensure that the DISA will have sufficient funds allocated to resolve the Y2K problem, it must place greater emphasis on estimating and accounting for Y2K costs.

Estimating Costs for Y2K. The DoD Management Plan suggests that DoD Components conduct a thorough review of resource requirements as part of their overall assessment of the Y2K problem. The plan emphasizes the importance of estimating Y2K costs by using cost factors. Further, the DoD Management Plan allows DoD Components to use any other accurate means to provide a realistic estimate of Y2K costs. However, the DoD and the Office of Management and Budget require estimated Y2K costs to be reported and, if the estimate is made by means other than the cost factors, the DoD Components must identify the methodology used. In addition, the DoD Management Plan suggests frequent updates of Y2K cost estimates as circumstances change.

DISA has not emphasized the development of Y2K-specific cost estimates. Of 24 management representatives, 16 had not attempted to estimate costs related to Y2K. DISA management representatives explained that they considered developing separate Y2K estimates to be unnecessary because Y2K-related costs would be covered by the normal system budgets for update, renovation, or modification. Furthermore, because Congress will not be providing additional funding for Y2K resolution, the DISA management representatives considered budget estimation for Y2K to be unnecessary and time-consuming. DISA must place a greater emphasis on cost estimates with frequent adjustments to keep them current, or it may find that unidentified testing costs will increase the overall Y2K estimated cost.

Accounting for Y2K Costs. The DoD Management Plan also emphasizes that Congress has requested and will continue to pursue an aggressive total accounting of the cost of Y2K compliance, even though Congress plans no budgetary relief to accomplish the Y2K mission. Management representatives stated that DISA personnel report direct Y2K costs to the Defense Integration Support Tools database and report indirect costs to the DISA Comptroller. Because DISA tracks costs separately, the congressional intent to obtain the actual Y2K program costs is not adequately being met.

Contingency Plans

The DISA has not developed contingency plans for each of its mission-critical systems.

Definition of Contingency Plan. A contingency plan is a strategy for responding to the loss of a system because of a disaster, such as flood, fire,

computer virus, or major software failure. The DoD Management Plan strongly emphasizes that DoD Components develop realistic contingency plans that include the following:

- developing and activating manual or contract procedures to ensure the continuity of core processes.

- developing procedures for emergency response, backup, and post-disaster recovery.

- developing contingencies in case a data exchange fails to take place as expected from an outside source.

- developing expenditures of additional funds to correct any unforeseen problems.

Furthermore, the DoD Management Plan recommends that DoD Components start the contingency plan in the assessment phase and update them during each subsequent phase.

DISA Contingency Plan. In our sample, 27 of 30 DISA systems that would continue to be active in the year 2000 did not have a written contingency plan to support operations in case the Y2K solutions failed. The DISA Y2K program manager explained that DISA will not start contingency planning until October 1, 1998. The program manager contends that contingency planning before program implementation will take critical manpower away from the Y2K problem resolution.

Importance of Contingency Planning. Preparing contingency plans is an essential element of risk management; they should be prepared from the perspective of the business area as well as from the perspective of the system owners and users. The DoD Management Plan states that contingency plans for the year 2000 are much more important than plans for routine system development or maintenance efforts, for which schedule slippages are nonfatal and common. The Y2K program must be completed on time. Without researching the contingencies that are available in case of Y2K system failure, management representatives as well as system users cannot effectively prioritize the efforts required to resolve the Y2K problems.

Testing and Compliance Checklists

DISA may have inappropriately reported systems to the Office of the Secretary of Defense as Y2K compliant. The classification of most of the systems reported as Y2K compliant was not supported by a signed compliance checklist or an acceptable equivalent. Systems should not be moved from the validation phase until they are fully tested and certified as Y2K compliant.

Compliance Checklists. The DoD Management Plan states that DoD Components should develop and document test-and-compliance plans and schedules for each converted or replaced application or system component. It also provides a checklist containing items to be included in the Y2K testing-and-compliance process that helps determine whether a system is compliant. The checklist is an aid for system owners to ensure that their systems are thoroughly tested and properly documented before they are considered to be Y2K compliant.

Y2K Compliant Systems. In January 1998, DISA reported that 21 of 98 mission-critical systems were Y2K compliant, and 49 of 127 non-mission-critical systems were Y2K compliant. In our sample, we looked at 13 systems that DISA considered Y2K compliant and found 10 systems that had been classified as Y2K compliant without being tested, without interface identification being made for those systems, and without the compliance checklists being completed.

DISA has developed a Y2K-compliance certification plan that provides instructions for determining the compliance of information technology, software, and systems that face a Y2K problem. The compliance certification plan also provides the steps necessary to determine whether modified information technology systems can ensure a smooth transition from the 20th century to the 21st century. Systems that are deemed properly modified will be certified as Y2K compliant. In addition, the compliance certification plan requires certifications from the test manager, system manager, and system customer for each compliance checklist. The DISA is also developing an applications Y2K test bed to provide testing for in-house-generated database applications.

Continuing DISA Actions

DISA is resolving several of the issues addressed in this report. The DISA Y2K program manager is revising the DISA Y2K Management Plan, which will be available for coordination within the DISA Directorates by June 30, 1998. DISA is also writing separate instructions for DISA Year 2000 Certification and Validation Guidance, which incorporates the DoD checklist on compliance and validation and a directive addressing risk management and contingency planning.

Other Matters of Interest

In a separate review, the Inspector General, DoD, is also examining the Y2K posture of the Defense Megacenters that DISA owns and operates. These organizations provide mainframe data processing services to functional users in

the Services and the Defense Agencies. Defense Megacenter Y2K concerns have been tentatively identified in the areas of reporting, testing, and contingency planning.

Conclusion

Although DISA has recognized the importance of solving Y2K problems in its systems, it has not emphasized the planning and precautionary strategies that are outlined in the DoD Management Plan to ensure that DISA will be well-positioned to deal with unexpected problems and delays. Unless DISA takes additional measures, it faces a high risk that its mission capabilities and those of supporting DoD Components will be impaired because of Y2K-related disruptions.

Recommendations, Management Comments, and Audit Response

We recommend that the Director, Defense Information Systems Agency:

1. Review changes to the DoD Year 2000 Management Plan, and update the Defense Information Systems Agency Year 2000 Management Plan according to those changes.

2. Disseminate the regulations, procedures and strategies governing the DoD Year 2000 Management Plan and the Defense Information Systems Agency Year 2000 Management Plan and other guidance to the operating levels.

3. Require system managers to accurately document the system status in accordance with the exit criteria prescribed in the DoD Year 2000 Management Plan.

4. Complete the identification of all interfaces and communicate the resolutions of the potential year 2000 interface problems to the interface partners.

5. Refine cost estimates for each system to determine the funding needed.

6. Develop contingency plans for mission-critical systems that will not complete the "implementation" phase by December 1998.

7. Determine systems as year-2000 compliant only after testing and completing the compliance checklists.

Management Comments. The Inspector General, Defense Information Systems Agency, generally concurred with the recommendations and described ongoing actions to implement them. Management will update the DISA Y2K Management Plan to reflect DoD guidance and requirements. Interfaces with both internal and external systems will be identified, and interface agreements will be documented through memorandums of agreement or interface control documents. Management stated that DoD agreed to exempt communications transport systems from developing formal interface agreements because adherence to applicable international and national standards accomplishes the same results. Using the revised guidance in the draft DoD Y2K Management Plan, DISA is revalidating Y2K cost estimates but does not anticipate needing any additional funding. Contingency plans will be developed for mission-critical systems that will not be fully Y2K compliant by September 30, 1998, or that will not be fully implemented by December 1998. Management also stated that Version 2.0 of the DISA Y2K Management Plan specifically requires that DISA complete a Y2K Compliance Checklist for all systems during the testing phase.

DISA management partially concurred with our recommendations related to dissemination of Y2K guidance and requirements and to documenting system status as prescribed in the DoD Y2K guidance. Management stated that DISA has used and continues to use every means possible to disseminate Y2K guidance. In November 1996, the draft DISA Y2K Management Plan, specific guidance from DoD and DISA management, and other important Y2K information was distributed via electronic mail to about 50 managers and Y2K points of contact. Additionally, information on Y2K web sites, and commercial and government software and hardware, are sent to Y2K points of contact and operating level personnel on an almost daily basis. Further, Y2K-related information is distributed during frequent Y2K status and progress reviews. Management stated that the system-status and milestone-events information in Appendix B of this report is so outdated that the current Y2K status of DISA is inaccurate. Currently, exit criteria for the renovation phase are nearly completed, and test schedules and validation plans for DISA mission-critical systems are being finalized. The status of DISA systems was intensely reviewed in April 1998 and is updated monthly. The complete text of management comments is in Part III of this report.

Audit Response. We consider management comments to be generally responsive to all recommendations. We also recognize that DISA has significantly improved its Y2K program and has made progress in remedying its Y2K problems since the audit. However, we could not verify DISA comments that DoD officials had agreed to exempt telecommunications transport systems from developing specific Y2K interface agreements. The present draft Version 2.0 of the DoD Management Plan does not provide such an exemption, and the staff in the Office of Year 2000 Oversight and Contingency Planning was not aware of any plans to include such a provision. We request that DISA clarify requirements for establishing interface agreements for telecommunications transport systems with DoD Y2K officials and provide comments on this aspect of the final report, including estimated completion dates for any planned actions, by September 4, 1998.

This Page Intentionally
Left Blank

Part II - Additional Information

Appendix A. Audit Process

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 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 progress that DISA has made in resolving the Y2K computing issue. The review included interviews conducted with 24 management representatives who are responsible for making 35 DISA systems Y2K compliant. Also, we evaluated documentation supporting actions taken to resolve Y2K deficiencies within specific DISA systems. We compared the DISA Y2K efforts with those described in the DoD Management Plan issued by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in April 1997. We assessed the efforts related to the progression of the 35 DISA systems reported in detail in Part I through the five-phase management process, using documents that included Office of Management and Budget guidance, the DoD Management Plan, the DISA Y2K Management Plan, DISA Y2K Test and Validation Guidelines, and systems inventory database information.

DoD-Wide Corporate Level Government Performance and Results Act (GPRA) Goals. In response to the GPRA, 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 war fighting capabilities. **(DoD-3)**

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

- **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. The General Accounting Office (GAO) has identified several high-risk areas in the DoD. This report provides coverage of the Information Management and Technology high-risk area.

Methodology

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from October 1997 through March 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 or statistical sampling procedures for this audit.

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

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognizes the Y2K issue as a material management control weakness area in the FY 1997 Annual Statement of Assurance.

Prior Coverage

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

Appendix B. Summary of Defense Information Systems Agency Systems Reviewed

System Name	Knowledge of Management Plan	Documented Y2K Strategies	Completed Interface Identification	Completed Interface Agreements[1]	Cost Estimates Reported	Documented Contingency Plans	Certified as Y2K Compliant[2]
Advanced Defense Red Switch Network Integrated Management Support System[3]	No	No	Yes	No	No	No	Yes
Anti-Drug Network[3]	No	No	Yes	No	No	No	N/A
Airfields Database[3]	No	No	Yes	No	No	No	Yes
Automated Resources Management System[3,4]	Yes	No	Yes	No	Yes	No	Yes
Communications Management and Control Activity Automated Billing System	Yes	Yes	Yes	No	No	No	Yes
Corporate Database for Windows[3]	Yes	No	N/A	N/A	No	No	Yes
Counter Drug Intelligence System[3]	No	Yes	Yes	No	No	Yes	N/A
Defense Information Systems Agency Acquisition Bulletin Board System[5]	Yes	No	N/A	N/A	Yes	No	No
Database Commitment Accounting System for Windows[5]	Yes	No	Yes	N/A	No	No	Yes
Defense Information Infrastructure-Common Operating Environment	Yes	Yes	No	No	No	No	No
Defense Information System Network[3]	No	No	Yes	No	Yes	No	No
Defense Information System Network-Asynchronous Transfer Mode[3]	No	No	Yes	No	Yes	No	Yes
Defense Information System Network Channel Service Unit and Data Service Unit[3]	No	No	Yes	No	Yes	No	Yes

Appendix B. Summary of Defense Information Systems Agency Systems Reviewed

System Name	Knowledge of Management Plan	Documented Y2K Strategies	Completed Interface Identification	Completed Interface Agreements[1]	Cost Estimates Reported	Documented Contingency Plans	Certified as Y2K Compliant[2]
Advanced Defense Red Switch Network Integrated Management Support System[3]	No	No	Yes	No	No	No	Yes
Anti-Drug Network[3]	No	No	Yes	No	No	No	N/A
Airfields Database[3]	No	No	Yes	No	No	No	Yes
Automated Resources Management System[3,4]	Yes	No	Yes	No	Yes	No	Yes
Communications Management and Control Activity Automated Billing System	Yes	Yes	Yes	No	No	No	Yes
Corporate Database for Windows[3]	Yes	No	N/A	N/A	No	No	Yes
Counter Drug Intelligence System[3]	No	Yes	Yes	No	No	Yes	N/A
Defense Information Systems Agency Acquisition Bulletin Board System[5]	Yes	No	N/A	N/A	Yes	No	No
Database Commitment Accounting System for Windows[3]	Yes	No	Yes	N/A	No	No	Yes
Defense Information Infrastructure-Common Operating Environment	Yes	Yes	No	No	No	No	No
Defense Information System Network[3]	No	No	Yes	No	Yes	No	No
Defense Information System Network-Asynchronous Transfer Mode[3]	No	No	Yes	No	Yes	No	Yes
Defense Information System Network Channel Service Unit and Data Service Unit[3]	No	No	Yes	No	Yes	No	Yes

System Name	Knowledge of Management Plan	Documented Y2K Strategies	Completed Interface Identification	Completed Interface Agreements[1]	Cost Estimates Reported	Documented Contingency Plans	Certified as Y2K Compliant[2]
Global Command and Control System	Yes	No	No	No	No	No	No
Global Combat Support System	Yes	Yes	No	No	No	No	No
Global On-line Marine Edit and Report System	No	No	Yes	No	Yes	No	No
Integrated Resource Management System	No	Yes	Yes	No	No	No	Yes
Mission Requirements Program[6]	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Nuclear Planning and Execution System[9]	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Pass Ultra Programmable[4]	Yes	No	No	No	No	No	No
Telecommunication Service Priority[4/5]	No	No	N/A	N/A	No	Yes	Yes
White House Communications Agency Property Book System	Yes	Yes	No	No	No	No	No
Warehouse Inventory System[8]	N/A	N/A	N/A	N/A	N/A	N/A	N/A

[1] Not applicable responses refer to those systems that do not have any external interfaces or internal interfaces.
[2] Responses of not applicable refer to those systems that are not beyond the renovation phase.
[3] Telecommunications transport system requiring waiver/exemption.
[4] Replacement system or system scheduled to be replaced.
[5] Stand alone systems.
[6] System owned by the National Security Agency.
[7] Initially identified as being in the renovation phase but the system was retired in July 1997.
[8] Retired.
[9] System transferred to the Air Force and Air Force expects the system to be implemented by January 1999.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Year 2000 Oversight and Contingency Planning Office
Assistant Secretary of Defense (Health Affairs)
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

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

Department of the Navy

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

Department of the Air Force

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

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligency Agency
Director, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency

Non-Defense Federal Organizations and Individuals

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:

  Special Committee on the Year 2000 Technology Problem
  Senate Committee on Appropriations
  Senate Subcommittee on Defense, Committee on Appropriations
  Senate Committee on Armed Services
  Senate Committee on Governmental Affairs
  House Committee on Appropriations
  House Subcommittee on National Security, Committee on Appropriations
  House Committee on Governmental 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

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

Inspector General

26 June 1998

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Director, Acquisition Management

SUBJECT: Comments to DODIG Draft Audit Report on DISA's Year 2000 Program

Reference: DODIG Draft Report, Audit on Management of the Defense Information Systems Agency Year 2000 Program (Project No. 8AS-0005), 27 May 1998

1. The Year 2000 Problem has been and continues to be the Director's Number 1 priority, especially for the mission critical systems. It has received increased top management visibility weekly since October 1997, when the Vice Director started chairing the DISA Y2K Weekly Updates. Prior to that date, the Director held several in-process reviews and the Chief Information Officer held monthly reviews.

2. While DISA concurs with the recommendations of the referenced report, we note that DISA has made tremendous progress since the audit observations were made and most of the recommended actions are well underway.

3. The point of contact for this action is Mr. Thomas J. Nicholas, Special Assistant to the IG for Y2K. He can be called at (703) 607-6315 or by email at nicholat@ncr.disa.mil.

FOR THE DIRECTOR:

1 Enclosure a/s

RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

MANAGEMENT COMMENTS TO DODIG DRAFT AUDIT REPORT ON MANAGEMENT OF THE DEFENSE INFORMATION SYSTEMS AGENCY YEAR 2000 PROGRAM (Project No. 8AS-0005)

The DODIG recommends that the Director, Defense Information Systems Agency:

1. Review changes to the DoD Year 2000 Management Plan, and update the Defense Information Systems Agency Year 2000 Management Plan according to those changes.

DISA Response: Concur. As noted in the draft report we will issue Version 2.0 DISA Year 2000 Problem Management Plan by 30 June 1998 at the end of our Renovation Phase. It is based on the latest draft of the DoD Year 2000 Management Plan, which is expected to be final before 30 June 1998.

2. Disseminate the regulations, procedures and strategies governing the DoD Year 2000 Management Plan and the Defense Information Systems Agency Year 2000 Management Plan and other guidance to the operating levels.

DISA Response: Partially concur. Downward communication is a vital part of any effort. However, DISA has used and continues to use every means possible to disseminate Y2K guidance to Program Managers and others. Drafts of the DISA Y2K Problem Management Plan, specific guidance from DOD and management, and other important documents were distributed to about 50 managers and Y2K Points of Contact via email in November 1996. The first DOD Y2K Management Plan was distributed in April 1997.

References to Y2K web sites, information on commercial and government off-the-shelf (COTS/GOTS) software and hardware, test results, and the latest guidance on Y2K have been disseminated to the Y2K points of contact and operating level personnel via email on a daily basis. Moreover, both weekly and monthly meetings have served to keep DISA staff and operating managers apprised of the problems and the progress of our Y2K challenge. Weekly Y2K updates have been held with the Vice Director, Chief of Staff, and senior managers since October 1997. These frequent Y2K progress review meetings of the key management officials and Y2K Coordinators also serve as a forum to distribute the latest and most relevant reports, schedules, and Y2K

guidance documents. Subsequently, this data along with certification and testing guidance is formally placed on the DISA/DoD/JITC and other relevant web pages. The draft DoD and draft DISA Year 2000 Management Plans were distributed via electronic mail in March 1998 to all Program Managers, Y2K Points of Contact, and other DISA system representatives. The final versions will be disseminated in a similar fashion and copies will be placed on the DoD and/or DISA web pages.

3. Require system managers to accurately document the system status in accordance with the exit criteria prescribed in the DoD Year 2000 Management Plan.

DISA Response: Partially concur. However, the data in Appendix B to this report is now so outdated that it gives an inaccurate picture of the DISA's true Y2K status at the end of June 1998. Continuous monitoring of systems progress through the phases has been occurring and reported as a standard feature of the Y2K weekly management briefing to the Vice Director and Chief of Staff. In addition, an accurate track record is kept of the progress of each system from one phase to the next. At this time, exit criteria for the Renovation Phase are nearly completed for almost all systems. Test schedules and validation plans are being finalized for DISA's mission critical systems. In addition, new DOD and DISA reporting requirements call for step by step updates on the status of Y2K by phase. The status of DISA mission critical and support systems was scrubbed in April 1998 and is being updated monthly.

4. Complete the identification of all interfaces and communicate the resolutions of the potential, Year 2000 interface problems to the interface partners.

DISA Response: Concur. Complete identification and documentation of interfaces and interface agreements has been underway since our initial inventory in 1996. DISA has identified internal system interfaces during the assessment phase; however, identification of external interfaces has taken longer. Nevertheless, this is an ongoing effort as our systems and networks are dynamic and the number of interfaces change frequently. Documentation of the Y2K compliance of the interfaces may take the form of applicable international and national standards, interface control documents, or memoranda of agreement (MOA),

depending on the nature of the interface. In the case of the Global Command and Control System (GCCS) we have identified 20 external interfaces that have potential Y2K impacts and we are preparing MOAs for each one. We expect to complete our documentation efforts by 30 June 1998, the current DOD milestone. DISA obtains recurring reports on the status of interfaces from system managers and presents progress reports to the Vice Director at the weekly Y2K management meeting.

To assist DISA in the interface identification effort, the DODIG is requested to follow up on its concurrence that "formal interface agreements for telecommunications systems may not be appropriate" (page 9, Par 1). DOD has agreed to include guidance in their next Year 2000 Management Plan making an exception for systems such as telecommunications transport systems where interface agreements are not appropriate because national and international standards appropriately define the interface.

Page 8
Paragraph 4

5. Refine cost estimates for each system to determine the funding needed.

DISA Response: Concur. However, no additional funding is anticipated or needed. Recovery of the cost of Year 2000 efforts already undertaken, in order to then carry our the original planned enhancements to our systems, would be extremely beneficial. We are presently revalidating the cost estimates for remediation of our Mission Critical systems using the revised guidance in the draft DOD Y2K Management Plan. All of the Y2K Points of Contact have been tasked to document their Y2K cost estimates. We will have a better total cost estimate by 1 July 1998.

6. Develop contingency plans for mission-critical systems that will not complete the "implementation" phase by December 1998.

DISA Response: Concur. All mission critical systems that will not complete full Y2K compliance by September 30, 1998, or full implementation by December 1998, will have a system contingency plan developed by December 1998.

7. Determine systems as year 2000 compliant only after testing and completing the compliance checklists.

DISA Response: Concur. Version 2.0 of the DISA Year 2000 Problem Management Plan requires that a DISA Y2k Compliance Checklist be completed for all DISA systems that were renovated, or that replace prior systems, during the Validation Phase. Our concentration has been on fixing Y2K problems in computation or interchange in our mission critical systems, as quickly as possible, so that our customers can build on our solutions, while continuing to meet the warfighter's needs. The paperwork was left to the Validation Phase when a more complete set of Year 2000 compliance criteria were available and the documentation requirements were more firmly set.

Audit Team Members

This report was prepared by the Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD.

Thomas F. Gimble
Patricia A. Brannin
Mary Lu Ugone
James W. Hutchinson
JoAnn Henderson
Hugh G. Cherry
Kathleen Fitzpatrick
Jennifer L. Zucal
Labib A. Baltagi
Sonya M. Mercurius
Wendy Stevenson
Krista S.Gordon

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Management of the Defense Information Systems Agency Year 2000 Program

B. DATE Report Downloaded From the Internet: 09/14/99

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 09/14/99**

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.