Audit Report

YEAR 2000 CERTIFICATION OF MISSION-CRITICAL
DOD INFORMATION TECHNOLOGY SYSTEMS

Report No. 98-147 June 5, 1998

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932 or visit the Inspector General, DoD, Home Page at: WWW.DODIG.OSD.MIL.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

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

Defense Hotline

To report fraud, waste, or abuse, contract 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

Y2K	Year 2000

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

June 5, 1998

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)

SUBJECT: Audit Report on Year 2000 Certification of Mission-Critical DoD Information Technology Systems (Report No. 98-147)

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

DoD Directive 7650.3 requires that all recommendations be resolved promptly. We request you to provide planned actions and completion dates for the recommendations by July 6, 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 D for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-147 **June 5, 1998**
(Project No. 8AS-0011)

Year 2000 Certification of Mission-Critical DoD Information Technology Systems

Executive Summary

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

The year 2000 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 next century.

Audit Objectives. Our objective was to determine whether the year 2000 certification process is adequate to ensure that mission-critical DoD information technology systems will continue to operate properly after the year 2000. Specifically, the audit examined DoD management policy and guidance relevant to certifying information technology systems as year 2000 compliant. The audit also evaluated the year 2000 certification process of selected mission-critical DoD information technology systems as implemented by the DoD Components.

Audit Results. DoD Components are not complying with year 2000 certification criteria before reporting systems as compliant. Of the 430 systems that DoD reported as year 2000 compliant in November 1997, we estimate that DoD Components certified only 109 systems (25.3 percent) as year 2000 compliant. As a result, DoD management reported as year 2000 compliant systems that have not been certified. More important, mission-critical DoD information technology systems may unexpectedly fail because they were classified as year 2000 compliant without adequate basis. The results are based on a randomly selected sample of 87 systems that DoD had reported as year 2000 compliant. Our statistical sampling methodology is described in Appendix A. A signed year 2000 compliance checklist was requested for each of the systems selected. See Part I for details of the audit results.

Summary of Recommendations. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) clarify certification requirements to include verification and validation, issue clear year 2000 quarterly

reporting requirements, and develop guidance for signature by the Deputy Secretary of Defense that directs DoD Components to establish oversight processes and procedures to enforce the requirements established in the other recommendations.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with the draft recommendations, stating that management currently is updating the Management Plan and must update the reporting requirements quarterly. Additionally, management will propose actions by the Deputy Secretary of Defense to clarify the importance of year 2000 compliance and the enforcement of reporting and evaluation requirements. See Part I for a summary of management comments and Part III for the complete text of the comments.

Audit Response. Management concurred with the recommendations but did not provide the specific actions to be implemented. Management stated that the Management Plan would be updated but did not discuss how the updated Management Plan would clarify year 2000 certification requirements. Management stated that the reporting requirements must be updated quarterly to comply with the latest Office of Management and Budget guidance but did not state that the guidance would be modified to prevent future occurrence of the errors that we identified in the report. Because of the time sensitivity of the year 2000 issue, the guidance on certification requirements needs to be effective immediately. Because the release date for the Management Plan update is unknown, an alternative solution may be to issue separate guidance on the certification process to be effective immediately. We request that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provide specific actions and associated completion dates for the guidance on certification requirements, quarterly reporting requirements, and the oversight process by July 6, 1998.

Table of Contents

Executive Summary i

Part I - Audit Results

Audit Background 2
Audit Objectives 5
Year 2000 Certification of Mission-Critical DoD Information Technology Systems 6

Part II - Additional Information

Appendix A. Audit Process
Scope and Methodology 16
Statistical Sampling Methodology and Sampling Results 17
Appendix B. Summary of Prior Coverage 19
Appendix C. Certification and Testing Results for Mission-Critical DoD Information Systems Audited 21
Appendix D. Report Distribution 24

Part III - Management Comments

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments 28

Part I - Audit Results

Audit Background

Year 2000 Date Processing Problem. 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 next century. The Y2K problem is rooted in the way that dates are recorded and computed in automated information systems. For the past several decades, systems have typically used two digits to represent the year, such as "97" representing 1997, to conserve electronic data storage and to reduce operating costs. With the two-digit format, however, the year 2000 is indistinguishable from 1900, or 2001 from 1901, and so forth. 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 following 1999. Calculation of Y2K dates is further complicated because the year 2000 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. In addition, 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.

As of November 1997, DoD reported 3,143 mission-critical systems* to the Office of Management and Budget. The total cost of the DoD Y2K effort was estimated at about $1.5 billion.

Department of Defense Year 2000 Management Plan. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued the "DoD Year 2000 Management Plan" (Management Plan) in April 1997. The Management Plan provides the overall DoD strategy and guidance for inventorying systems, prioritizing systems, retiring systems, and monitoring progress. The Management Plan makes the DoD Components responsible for implementing the five-phase Y2K management process. The goal is to have all DoD systems certified as Y2K compliant and implemented no later than November 1, 1999.

The DoD Five-Phase Management Process. Each of the five phases is supported by program and project management and represents a major Y2K

*When a mission-critical system's capabilities are degraded, the organization

program activity or segment. The April 1997 Management Plan shows the following target completion dates for the five phases ranging from December 1996 through November 1, 1999.

• Phase I - Awareness. Awareness, education, and initial organization and planning take place. Target completion date: December 1996.

• Phase II - Assessment. Scope of Y2K effects is identified, and system-level analysis takes place. Target completion date: June 1997.

• Phase III - Renovation. Required system renovations are accomplished. Target completion date: December 1998.

• Phase IV - Validation. Systems are certified as Y2K compliant as a result of various testing and compliance processes. Target completion date: January 1999.

• Phase V - Implementation. Systems are fully operational after being certified in Phase IV. Target completion date: November 1, 1999.

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) is in the process of issuing an updated Management Plan, which further accelerates the target completion dates for the Renovation, Validation, and Implementation phases, resulting in a completion date of December 1998.

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 all corrective actions to all systems. The new target completion dates are September 1998 for the Renovation phase and January 1999 for the Validation phase.

Certification. The 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 Management Plan, a system is certified when the system manager signs a Y2K compliance checklist. An example of a Y2K compliance checklist is in Appendix B of the Management Plan. The purpose of the checklist is to assist system managers in ensuring that their systems are Y2K compliant.

Testing. The Management Plan states that a validation schedule should be developed for all systems during the assessment phase and that validation should be completed as soon as possible. Validation, according to the Management Plan, includes evaluating the system to determine whether it is Y2K compliant. Also during the assessment phase, every piece of code should be examined to determine whether any two-digit date handling is involved. According to the Management Plan, DoD Components should develop and document test and compliance plans and schedules for each converted or replaced application or system component. Additionally, DoD Components are responsible for determining whether the vendor software is Y2K compliant. DoD Components must also ensure that the contractor-converted systems are tested.

Year 2000 Guidance Developed by DoD Components. The Army, the Air Force, the Defense Logistics Agency, and the Defense Information Systems Agency each issued internal Y2K guidance to address the Y2K problem. Each guidance package requires a compliance/certification checklist to be completed and testing to be done. The Washington Headquarters Services, the Defense Special Weapons Agency, the Defense Finance and Accounting Service, and the Assistant Secretary of Defense (Health Affairs) use the Management Plan for Y2K guidance.

Army. The Army "Project Change of Century Action Plan, Revision I," October 4, 1996, provides the Army strategy and management approach for addressing the Y2K problem. The Army plan requires system developers or maintainers and the system's functional proponent to certify and document each system's Y2K compliance. According to the Army plan, testing must include regression testing, integrated testing, and simulated Y2K testing. The Army compliance checklist guidance dated June 1997 states that a system or device is not considered Y2K compliant until positive results have been achieved in accordance with compliance levels outlined in Section 10 of the Army plan checklist. The checklist is required for each Army system that has been reported to the Army year 2000 database. The checklist is required for systems previously assessed and found to be compliant, systems that contain no date information, and systems with no Y2K impact.

Air Force. The Air Force "Year 2000 Guidance Package," April 1, 1997, describes the Air Force Y2K management issues and the five-phase resolution process. The guidance states that system owners, users, designers, and developers should not assume that any system is Y2K compliant until it has been "extensively analyzed using proven methods." The Air Force requires that every system classified as Y2K compliant have incorporated the compliance checklist in the validation process. The Air Force believes that completing the checklist will not guarantee that a system will be Y2K compliant, but that the checklist will give system managers a "tremendous start in their certification efforts." The guidance states that each system should be certified as Y2K compliant after testing is complete, and it recommends the use of independent testing or validation organizations.

Defense Logistics Agency. The Defense Logistics Agency "Year 2000 AIS [Automated Information System] Certification Guidance," October 27, 1997, defines the conditions that must be met for an automated information system to be considered Y2K compliant. The guidance states that the Y2K certification checklist is to be completed during testing. The Y2K certification checklist "only indicates potential readiness for the functional area to start functional testing." The Y2K certification checklist is formally completed during functional testing. The completed checklist is sent to the Year 2000 Program Office to update the certification status.

Defense Information Systems Agency. The "Defense Information Systems Agency Year 2000 Testing Guideline," November 12, 1997, provides the strategy for all systems that require Y2K testing by the Defense Information Systems Agency. The guidance states that it can be used for all DoD systems to "provide reasonable assurance that the Y2K problem has been resolved." The

guidance states that tested systems are deemed compliant if they meet the compliance requirements in the Management Plan. The guidance states that Y2K test results should be used to determine whether the system is compliant. The guidance also states that the Defense Information Systems Agency's goal is to ensure that the systems are Y2K compliant "by providing a rigorous Y2K test management approach."

On January 22, 1998, the Vice Director of the Defense Information Systems Agency issued a memorandum recommending that central design activities (organizations that design and produce software that is used on a DoD Component-wide or DoD-wide basis) specifically qualify Y2K testing results to help avert potential legal liabilities. The suggested disclaimer provides no guarantee that any information technology product that passed Y2K compliance testing is actually Y2K compliant.

Audit Objectives

Our objective was to determine whether the Y2K certification process is adequate to ensure that mission-critical DoD information technology systems will continue to operate properly after the year 2000. Specifically, the audit examined DoD management policy and guidance relevant to certifying information technology systems as Y2K compliant. The audit also evaluated the Y2K certification process of selected mission-critical DoD information technology systems as implemented by the DoD Components. See Appendix A for a discussion of the audit scope and methodology.

Year 2000 Certification of Mission-Critical DoD Information Technology Systems

Based on a randomly selected sample of 87 out of 430 systems that DoD reported as Y2K compliant in November 1997, we estimate that DoD Components certified only 109 (25.3 percent) of the 430 systems as Y2K compliant. Although the Management Plan contains guidance regarding Y2K certification, the DoD Components did not certify the majority of the sampled systems reported as Y2K compliant.

Systems were not certified because DoD Components did not adequately implement and enforce the guidance in the Management Plan or their own Y2K guidance. Additionally, the Management Plan is not consistently clear as to specific Y2K certification requirements.

As a result, DoD management reported as Y2K compliant systems that have not been certified. More important, mission-critical DoD information technology systems may unexpectedly fail because they were classified as Y2K compliant without adequate verification and validation.

DoD Year 2000 Guidance

Y2K Status Reporting. The DoD Components are required to report quarterly to the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) the Y2K status of their mission-critical systems. In turn, the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provides the results to the Office of Management and Budget. In November 1997, DoD reported that 430 DoD mission-critical systems (excluding 242 systems from DoD intelligence organizations) were Y2K compliant. The following table shows the number of systems reported as Y2K compliant for each DoD Component.

Y2K Compliant Mission-Critical Systems: November 1997

Component	Number of Y2K Compliant Systems
Assistant Secretary of Defense (Health Affairs)	42
Department of the Army	188
Department of the Air Force	97
Defense Contract Audit Agency	1
Defense Finance and Accounting Service	12
Defense Information Systems Agency	14
Defense Logistics Agency	17
Defense Security Assistance Agency	1
Defense Special Weapons Agency	3
Washington Headquarters Services	55
Total	**430**

The Department of the Navy did not report any compliant systems for the November 1997 Quarterly Report.

DoD Year 2000 Certification Requirements and Process. The Management Plan states that system owners, users, designers, and developers cannot assume that any system is Y2K compliant until the system manager certifies it. According to the Management Plan, a system is not certified until the system manager signs a Y2K compliance checklist. The checklist is a tool for ensuring that the system manager has considered Y2K aspects. Those aspects include whether the system successfully processes data containing dates in the twentieth and twenty-first centuries and other indirect date usage, whether the system accurately recognizes and processes the year 2000 as a leap year and other internal usage of dates, and whether the DoD Component has identified external system interfaces and the type of date fields used by the system. The checklist also poses Y2K considerations if commercial software or software that the Government previously developed is used in the system. The Y2K guidance that the Army, the Air Force, the Defense Logistics Agency, and the Defense Information Systems Agency developed also requires the completion of a checklist.

Purpose of the Y2K Compliance Checklist. The overall intent of the Y2K compliance checklist is to help guide the system manager in ensuring that a system is Y2K compliant. A Y2K compliant system accurately processes and calculates date data from, into, and between the twentieth and twenty-first centuries and correctly recognizes leap years. Additionally, the system should successfully process data containing dates with no adverse effect on the application's functionality. The system manager should accomplish two vital steps before

certifying a system as compliant. The first step is verification that all potential Y2K impacts on the system were identified and, if necessary, that the selection and implementation of appropriate solutions were made. The second step is validation that any Y2K corrective actions are effective, and that the system accurately processes and calculates dates between centuries. Validation is normally performed through actual testing; the type of validation performed directly relates to the level of certification indicated on the checklist. Completion of the Y2K compliance checklist is not a guarantee of Y2K compliance; however, completion of the Y2K compliance checklist for each mission-critical system should provide senior management with an indicator and documented evidence that the system has been appropriately reviewed for potential Y2K impacts and that the necessary corrections were implemented.

Compliance With Year 2000 Certification Guidance

The level of compliance with Y2K certification requirements was low, and specific Y2K certification requirements were not uniformly clear. For each of the 87 systems randomly selected from the 430 systems that DoD had reported as Y2K compliant, we asked the designated point of contact for the certification date of the system and a copy of the Y2K compliance checklist. Our statistical sampling approach and methodology is described in Appendix A. We received answers to the questionnaire for 83 of the 87 systems.

Compliance With Certification Requirements. System representatives provided a copy of a Y2K compliance checklist, signed as of November 1997, for only 22 of the 83 systems that provided results in our sample. After allowing for the 4 systems for which we received no results, we concluded, with a 95-percent confidence level, that between 265 and 338 systems were not certified. Using the unbiased point estimate of 301 systems, we project that 70 percent of the systems reported as compliant in November 1997 did not complete a Y2K compliance checklist, which the system manager also signed as of November 1997.

Also, the existence of a completed and signed Y2K compliance checklist did not always mean that the system was Y2K compliant. The points of contact for 3 of the 22 systems in our sample with completed and signed checklists indicated that the systems were not fully Y2K compliant at the time that the checklist was signed. We also noted that the Management Plan does not clearly require that validation of Y2K compliance, such as testing systems impacted by dates, be completed before certification. The requirement in the Management Plan for certification is that the system manager signs the Y2K compliance checklist. Another 2 of the 22 systems in our sample certified as Y2K compliant were not validated and had "not applicable" for every answer on the checklist. DoD Components need to test systems impacted by dates to validate that the system is Y2K compliant. The Management Plan's Y2K certification process should state a clear requirement for validation, including testing for systems impacted by dates, or the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) should issue separate guidance on the certification process.

The Defense Finance and Accounting Service and the Defense Logistics Agency provided completed and signed checklists for all of their systems included in our sample. Appendix C presents the audit results for each of the sampled systems.

Clarity of Year 2000 Certification Guidance. The Management Plan does not clearly describe the certification process or specific requirements. For example, the Management Plan:

- states that system manager signature on the checklist constitutes certification, but does not prohibit the checklist from being signed before full Y2K compliance is achieved;

- does not clearly state that completion of the Y2K compliance checklist, or a similar checklist providing for Y2K verification and validation, is required before a system can be reported as Y2K compliant;

- does not define the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) or DoD Component-level oversight requirements or processes for DoD Y2K organizations and actions to ensure accurate Y2K reporting; and

- provides for a level of certification defined as "not certified or not certified yet." The legitimacy of certifying a system on that basis is not clear.

The purpose of the Y2K compliance checklist is to assist in ensuring that the system is Y2K compliant; however, system managers could complete and sign the checklist without the system being fully compliant or validated for compliance. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) should include requirements for compliance and validation in the certification process in the Management Plan. Currently, the only specific requirement for Y2K certification in the Management Plan is the system manager's signature on the Y2K compliance checklist. The Management Plan has been under revision for more than 6 months.

Year 2000 Testing of Mission-Critical Systems

Certification Levels. The Management Plan compliance checklist requires that each system representative indicate a level of certification. Some of the certification levels are keyed to the particular type of validation performed. For example, a system representative would indicate a certification level of "1" if the system was independently tested. A system would merit a level of "2" if an independent audit of the system and existing testing was performed. Although caution is provided that an assumption of higher risk is involved, several certification level "3" options are described for self-certification. The self-certification levels are not keyed to any particular type of testing.

Because self-certification can involve considerable risk to obtaining an objective validation that a system is Y2K compliant and because the certification level that the checklist in the Management Plan requires is not keyed to any particular type of validation, our questionnaire contained additional validation choices on which system managers could have based certification levels. We asked the point of contact for each system in our sample to select the most appropriate choice from our list of bases for certification.

Types of Y2K Validation Performed. Of the 83 systems that provided results in our sample, 32 were actually tested for Y2K compliance; 14 systems were inspected without testing (such as a manual review of the system's software code); 7 systems were considered Y2K compliant based on a statement from another organization; and 30 systems were considered Y2K compliant without testing, inspection without testing, or a statement from another organization regarding Y2K compliance. The Defense Finance and Accounting Service and the Defense Logistics Agency provided test results for all of their sampled systems. The points of contact for 17 of the 51 systems that did not undergo actual testing stated that they are currently testing or will test the systems in the future. The points of contacts for 2 of the 32 systems that were actually tested stated that they will perform additional testing of the systems.

We considered actual testing to be independent testing or organizational testing, with or without an independently verified process. However, we fully recognize that other types of validation may be an adequate basis for certification. For instance, software inspection may be adequate when the individual inspecting the software does not anticipate a date processing dependency, such as for software embedded in weapon systems. While embedded software probably measures elapsed time, the need to measure elapsed days in a combat scenario is not probable. The same assumption, however, cannot be made for software that supports a weapon system. For example, an aircraft maintenance system probably has date dependencies. The system points of contact for 6 of the 14 systems in our sample that were inspected without testing stated that the system did not use dates.

Although the Management Plan states that DoD Components should complete validation of the system as soon as possible, it does not clearly require system managers to validate Y2K compliance before certification of a system. Testing is the tool used to validate that a system impacted by dates will correctly process date and date-related data in the twentieth and twenty-first centuries. According to the Management Plan, DoD Components must test the individual applications, computer platforms, operating systems, utilities, applications, databases, and interfaces for Y2K compliance.

Of the 430 systems reported as compliant in November 1997, our sample results, which are detailed in Appendix A, showed that the majority did not undergo actual testing to validate Y2K compliance. Based on our sample results, we project the following:

- 158 (36.8 percent) of the 430 systems reported as compliant were actually tested for Y2K compliance.

- 69 (16.1 percent) of the 430 systems reported as Y2K compliant were determined to be Y2K compliant through an inspection of the system without testing.

- 35 (8 percent) of the 430 systems reported as Y2K compliant were classified as Y2K compliant based on statements from another organization. The Management Plan states that the DoD Component must determine whether the vendor software is Y2K compliant, and it must not accept vendor certification at face value.

- 148 (34.5 percent) of the 430 systems were reported as compliant without testing, inspection without testing, or a statement from another organization regarding Y2K compliance.

Four systems did not provide answers to our questionnaire. Therefore, the projection categories just listed do not total 430 systems, or 100 percent.

Impact on Accuracy of DoD Reports

The DoD Components did not correctly report many of the 87 systems selected from the 430 systems that DoD reported as Y2K compliant in November 1997. Inspector General, DoD, Report No. 98-077, "Year 2000 Computing Problem Reports: August 1997 Report," February 18, 1998, states that Y2K reporting definitions and procedures were not clear or well understood by DoD Components. Accordingly, the information that DoD provided to the Office of Management and Budget was not fully reliable. The results of this audit indicate that the requirements related to Y2K quarterly reporting are still not well understood or consistently complied with. For example:

- For 9 of the 87 systems in our sample, the points of contact indicated that the systems are no longer classified as mission-critical.

- For 13 of the 87 systems, the points of contact indicated that the systems were actually in a Y2K phase before implementation.

- For 4 of the 87 systems, the points of contact indicated that the systems were in the development stage, were not developed, or were not received.

- According to the point of contact, one Y2K compliant system in our sample was an office of people, not an automated system.

The primary purpose of the quarterly reports is to provide senior DoD and Federal Government managers with a tool to measure progress in the solving of the Y2K "problem." We noted that the number of systems that DoD reported in November 1997 as already Y2K compliant actually decreased by 91 systems (excluding DoD intelligence agencies) from the August 1997 report. We believe that the primary reason for that decrease in compliant systems is more conservative and realistic reporting by the DoD Components. While we applaud more accurate Y2K reporting, we also recognize that the decrease in Y2K compliant systems reported in November 1997 indicates that a baseline for measuring progress has yet to be established. Until DoD issues firm reporting guidance, we concluded that a stable and useful reporting baseline will continue to be elusive.

Conclusion

DoD is reporting systems as Y2K compliant that have not been appropriately certified or validated. Of the 430 systems reported in November 1997 as Y2K compliant, we project that only 109 were certified as Y2K compliant. Certification of Y2K compliance is required not only for accurate reporting, but also for providing DoD senior management with reasonable assurance that DoD automated systems will continue to operate correctly into the next century. The inappropriate reporting of systems as compliant may impede DoD from obtaining the necessary visibility to ensure a thorough and successful transition to Y2K compliance for all DoD systems. Without that smooth transition, DoD mission-critical information technology systems may unexpectedly fail because they were erroneously classified. The Y2K certification process should include clear requirements for compliance and validation, including testing for systems impacted by dates, to help ensure that mission-critical systems will not fail upon the turn of the century.

Sufficient time to fix the DoD Y2K "problem" is quickly running out. The year 2000 will arrive exactly on schedule. Senior DoD management cannot afford to make Y2K program decisions based on highly inaccurate information. If DoD does not take the action that it needs to obtain accurate information as to the status of its Y2K efforts, we believe that serious Y2K failures may occur in DoD mission-critical information technology systems.

Recommendations, Management Comments, and Audit Response

We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence):

1. Issue to DoD Components clarified DoD year 2000 certification requirements, to include specific verification and validation requirements, to be effective immediately.

2. Issue to DoD Components clear, firm year 2000 quarterly reporting requirements.

3. Develop guidance for the signature of the Deputy Secretary of Defense that directs DoD Components to establish oversight processes and procedures to effectively enforce the DoD requirements established in Recommendations 1. and 2.

Management Comments. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with our recommendations. Management currently is updating the Management Plan. Management stated that the reporting requirements must be updated quarterly and that our audit results will be used to improve the reporting instructions. Additionally, management will propose actions by the Deputy Secretary of Defense to clarify the importance of year 2000 compliance and the enforcement of reporting and evaluation requirements.

Audit Response. Although management concurred with the recommendations, management did not provide the specific actions to be implemented. Management stated that the Management Plan would be updated but did not discuss how the updated Management Plan would clarify year 2000 certification requirements. Management stated that the reporting requirements must be updated quarterly to comply with the latest Office of Management and Budget guidance but did not state that the guidance would be modified to prevent the errors we identified in the report from occurring in the future. Because of the time sensitivity of this year 2000 issue, the guidance on certification requirements needs to be effective immediately. Because the release date for the Management Plan update is unknown, an alternative solution may be to issue separate guidance on the certification process to be effective immediately. We request that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provide specific actions and associated completion dates for the guidance on the certification process, quarterly reporting, and the oversight process by July 6, 1998.

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 and Methodology

Work Performed. We reviewed and evaluated the DoD Year 2000 Management Plan issued by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in April 1997. We compared the Y2K guidance and compliance checklists issued by the Army, the Air Force, the Defense Logistics Agency, and the Defense Information Systems Agency with the Management Plan guidance and the Y2K compliance checklist. We distributed a questionnaire to the system representatives for 87 statistically selected systems from the 430 DoD mission-critical systems reported as compliant to determine the basis used for certifying the system as Y2K compliant. We performed an analysis of the questionnaire responses and evaluated the year 2000 certification process of selected mission-critical DoD information technology systems as implemented by the DoD Components.

Limitations to Audit Scope. The Management Plan requires external interfaces to be validated as Y2K compliant for the system to be certified as Y2K compliant. However, for the purpose of this audit, we asked questions regarding the specific system statistically selected; therefore, we did not ensure in all cases that external interfaces or operating systems for the specific audited system were compliant.

Use of Computer-Processed Data. No computer-processed data were used in the course of the audit.

Use of Technical Assistance. Assistance was provided by an Operations Research Analyst of the Quantitative Method Division of the Office of the Assistant Inspector General for Auditing, DoD. He assisted us in generating a random sample and projecting the results from our sample to the sample universe.

Audit Type, Dates, and Standards. We performed this program audit from December 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.

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. This report does present a material management control weakness. Specifically, the management controls are not adequate to ensure accurate quarterly reporting. However, separate reporting of that weakness is unnecessary.

Statistical Sampling Methodology and Sampling Results

Sampling Purpose. The purpose of the statistical sampling plan is to estimate the number of mission-critical DoD information technology systems that were certified or tested and those that were not certified or tested.

Universe Represented and Sampling Design. The table on page 7 of this report includes the universe data. The 430 systems were reported to the Office of Management and Budget as compliant by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in November 1997. We asked the system representatives for the statistically selected systems to answer a questionnaire regarding the date on which the system was certified and the basis for certification (such as testing, inspection, or certification by another organization). We randomly selected 87 systems from the sample universe.

Certification Sampling Results. Of those 87 systems, 22 systems were certified, 61 systems were not certified, and no results were received for 4 systems. Statistical projections of the results of systems certified and not certified are calculated over the universe by using 95-percent confidence levels. The projected results for certification are in Table A-1.

Table A-1. DoD Mission-Critical Systems Certified for Year 2000 Compliance

	Lower Bound	Point Estimate	Upper Bound
Certified	74	109	144
Not Certified	265	301	338
No Results	4	20	37

The above projections show that we are 95-percent confident that between 74 and 144 systems were certified. For the purpose of this report, we used the unbiased point estimate of 109 for the number of systems certified. The results can be interpreted similarly for the systems not certified and the systems with no results.

Projections for the total values for lower and upper bounds have been calculated independently and may not necessarily be the direct sum of two individual components.

Validation Sampling Results. Of the 87 sampled systems, 32 systems were tested for Y2K compliance, 14 systems were determined to be Y2K compliant

through an inspection of the system without testing, 7 systems were classified as Y2K compliant based on statements from another organization, 30 systems were not tested or inspected and did not obtain a statement from another organization regarding compliance, and 4 systems did not provide answers to the questionnaire. Statistical projections of the results of Y2K compliance validation are calculated over the universe by using 95-percent confidence levels. The projected results for testing are in Table A-2.

Table A-2. DoD Mission-Critical Systems Validated for Year 2000 Compliance

	Lower Bound	Point Estimate	Upper Bound
Tested	119	158	197
Inspected	40	69	99
Statements from another organization	13	35	57
No testing	110	148	187
No results	4	20	37

The above projections show that we are 95-percent confident that between 119 and 197 systems were actually tested for Y2K compliance. For the purpose of this report, we used the unbiased point estimate of 158 for the number of systems actually tested. The results can be interpreted similarly for the systems inspected, systems classified as Y2K compliant based on statements from another organization, systems not tested, and systems with no results.

Projections for the total values for lower and upper bounds have been calculated independently and may not necessarily be the direct sum of two individual components.

Appendix B. Summary of Prior Coverage

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

Inspector General, DoD

Inspector General, DoD, Report No. 98-077, "Year 2000 Computing Problem Reports: August 1997 Report," February 18, 1998. The report states that the DoD Component second quarter reports on the Y2K issue did not provide all the required information and were not fully reliable. Accordingly, DoD will not have an adequate baseline to effectively measure its Y2K progress. Additionally, DoD Components did not consistently interpret the Chief Information Officer reporting requirements. The Management Plan provides definitions for "system" and "mission-critical," but definitions are nonspecific and open to interpretation. Also, DoD did not establish clear reporting guidance and requirements. The report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), in the role of the DoD Chief Information Officer, update the DoD Year 2000 Management Plan to reflect changes in reporting requirements and include adequate procedures on how Y2K quarterly reports should reconcile. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred and stated that the DoD Y2K Management Plan would be updated accordingly.

Inspector General, DoD, Report No. 98-074, "Sharing Year 2000 Testing Information on DoD Information Technology Systems," February 12, 1998. The report states that DoD has designated the use of homepages on the Internet as the primary means of sharing Y2K related information, and DoD Components have made progress in establishing Y2K information on their respective homepages. However, the process for sharing Y2K testing information can be more effective. DoD Components may be inefficiently spending time-sensitive resources in solving the Y2K problem through the duplication of efforts and in attempting to locate accurate testing information. The ability to retrieve and use all appropriate testing information in a timely and efficient manner will be instrumental in the solution of the Y2K problem. The report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), as the DoD Chief Information Officer, establish a DoD-sponsored Y2K testing information center within DoD for gathering, analyzing, storing, and disseminating Y2K-related testing information and provide Y2K hotline services to the DoD Components. Further, the report recommended that DoD Components be notified of the testing center's Y2K role and responsibilities and of the DoD Components' responsibility to share testing information and that DoD internet homepages be

organized to enable users to quickly and easily access the center for Y2K testing information. Although the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with the recommendations, our intent was to establish a DoD-sponsored Y2K testing information center, recognized by the other DoD Components, to organize and provide links to the Y2K testing information provided on the internet by the DoD Components. Accordingly, we added recommendations to clarify the actions needed to sufficiently identify, publicize, and access sources of Y2K testing information. We requested comments on the additional recommendations.

Appendix C. Certification and Testing Results for Mission-Critical DoD Information Systems Audited

	No Testing[1]	Testing[2]	Certification by Another Organization[3]	Inspection Without Testing[4]	Certified[5]	Note[6]
Department of the Air Force						
1.	Yes	No	No	No	No	a
2.	Yes	No	No	No	No	c
3.	Yes	No	No	No	No	d
4.	Yes	No	No	No	No	a, d, e
5.	No	Yes	No	No	Yes	d
6.	No	Yes	No	No	Yes	
7.	No	Yes	No	No	Yes	
8.	Yes	No	No	No	No	e
9.	Yes	No	No	No	No	e
10.	Yes	No	No	No	No	e
11.	Yes	No	No	No	No	e
12.	Yes	No	No	No	No	e
13.	N/A[7]	N/A	N/A	N/A	N/A	g
14.	Yes	No	No	No	No	
15.	No	Yes	No	No	Yes	
16.	Yes	No	No	No	No	b, e
17.	Yes	No	No	No	No	a
18.	No	Yes	No	No	Yes	
19.	No	Yes	No	No	No	b, d
20.	Yes	No	No	No	No	a
21.	Yes	No	No	No	No	c
22.	No	No	No	Yes	No	
23.	No	Yes	No	No	No	
24.	No	Yes	No	No	Yes	
Department of the Army						
25.	No	No	No	Yes	No	f
26.	No	No	Yes	No	Yes	
27.	No	No	Yes	No	No	e
28.	Yes	No	No	No	No	
29.	Yes	No	No	No	No	d
30.	No	No	No	Yes	No	
31.	No	No	No	Yes	No	e
32.	Yes	No	No	No	No	
33.	No	No	Yes	No	No	
34.	Yes	No	No	No	No	a
35.	No	Yes	No	No	Yes	
36.	Yes	No	No	No	No	b
37.	No	Yes	No	No	No	
38.	No	Yes	No	No	Yes	
39.	No	No	Yes	No	No	a, e

Note: See the footnotes at the end of the appendix.

Appendix C. Certification and Testing Results for Mission-Critical DoD Information Systems Audited

	No Testing	Testing	Certification by Another Organization	Inspection Without Testing	Certified	Note
Department of the Army (cont'd)						
40.	No	Yes	No	No	No	e
41.	No	Yes	No	No	No	e
42.	Yes	No	No	No	Yes	h
43.	No	Yes	No	No	No	
44.	No	No	No	Yes	No	e
45.	No	No	No	Yes	No	d, f
46.	Yes	No	No	No	No	i
47.	No	No	No	Yes	No	e
48.	No	No	Yes	No	No	e
49.	N/A	N/A	N/A	N/A	N/A	d
50.	No	No	No	Yes	No	f
51.	Yes	No	No	No	No	
52.	No	Yes	No	No	Yes	
53.	No	Yes	No	No	Yes	
54.	Yes	No	No	No	No	
55.	No	No	Yes	No	No	
56.	No	No	Yes	No	No	
57.	Yes	No	No	No	No	a
58.	No	No	No	Yes	No	f
59.	No	No	No	Yes	No	f
60.	No	Yes	No	No	Yes	
61.	No	No	No	Yes	No	f
62.	Yes	No	No	No	No	a, e
63.	N/A	N/A	N/A	N/A	N/A	d
64.	N/A	N/A	N/A	N/A	N/A	d
Defense Finance and Accounting Service						
65.	No	Yes	No	No	Yes	
66.	No	Yes	No	No	Yes	
Defense Information Systems Agency						
67.	No	Yes	No	No	No	
68.	Yes	No	No	No	No	e
69.	No	Yes	No	No	No	
Defense Logistics Agency						
70.	No	Yes	No	No	Yes	
71.	No	Yes	No	No	Yes	
Defense Special Weapons Agency						
72.	No	No	No	Yes	No	
Assistant Secretary of Defense (Health Affairs)						
73.	Yes	No	No	No	No	
74.	No	Yes	No	No	No	
75.	No	No	No	Yes	No	

Note: See the footnotes at the end of the appendix.

	No Testing	Testing	Certification by Another Organization	Inspection Without Testing	Certified	Note
Assistant Secretary of Defense (Health Affairs) (cont'd)						
76.	No	Yes	No	No	No	
77.	No	Yes	No	No	Yes	
78.	Yes	No	No	No	No	e
Washington Headquarters Services						
79.	No	Yes	No	No	No	
80.	Yes	No	No	No	No	a
81.	No	Yes	No	No	Yes	
82.	No	No	No	Yes	No	
83.	No	Yes	No	No	No	
84.	Yes	No	No	No	No	b, e
85.	No	Yes	No	No	Yes	
86.	No	Yes	No	No	Yes	
87.	No	Yes	No	No	Yes	

[1]As of November 1997, the system was reported as compliant without testing, an inspection without testing, or a statement from another organization regarding Y2K compliance.
[2]The system was independently tested or tested by the DoD Component for Y2K compliance.
[3]The system was classified as compliant based on a statement from another organization.
[4]The system was inspected for ability to process data, but no testing was performed to determine Y2K compliance.
[5]The point of contact provided a Y2K compliance checklist signed as of November 1997.
[6]The following notes apply to the system at the time of the audit:

a. System is in the renovation phase.
b. System is in the validation phase.
c. System is under development.
d. System is no longer classified as mission-critical.
e. System is currently being tested or will be tested in the future.
f. Year 2000 dates do not impact the system.
g. Element is an office, not a system.
h. Software for system was not developed.
i. System had not been received by point of contact.

[7]Question not answered on questionnaire.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Deputy Under Secretary of Defense (Logistics)
  Director, Defense Procurement
  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)
  DoD Year 2000 Project Officer
Assistant Secretary of Defense (Health Affairs)
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

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

Unified Commands

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

Other Defense Organizations

Director, Ballistic Missile Defense Organization
  Chief Information Officer, Ballistic Missile Defense Organization
Director, Defense Advanced Research Projects Agency
  Chief Information Officer, Defense Advanced Research Projects Agency
Director, Defense Commissary Agency
  Chief Information Officer, Defense Commissary Agency
Director, Defense Contract Audit Agency
  Chief Information Officer, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
  Chief Information Officer, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
Director, Defense Legal Services Agency
  Chief Information Officer, Defense Legal Services Agency
Director, Defense Logistics Agency
  Chief Information Officer, Defense Logistics Agency
Director, Defense Security Assistance Agency
  Chief Information Officer, Defense Security Assistance Agency
Director, Defense Security Service
  Chief Information Officer, Defense Security Service
Director, Defense Special Weapons Agency
  Chief Information Officer, Defense Special Weapons Agency
Director, National Security Agency
  Inspector General, National Security Agency
Director, On-Site Inspection Agency
  Chief Information Officer, On-Site Inspection Agency
Director, Washington Headquarters Services
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency

Non-Defense Federal Organizations and Individuals

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

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

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Technology Problem
House Committee on Appropriations
House Subcommittee on National Security, Committee on Appropriations
House Committee on Government Reform and Oversight
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform and Oversight
House Committee on National Security

Part III - Management Comments

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

May 11, 1998

MEMORANDUM FOR DIRECTOR ACQUISITION MANAGEMENT, OIG

Subject: Audit Report on Year 2000 Certification of Mission-Critical DoD Information Technology Systems (Project No. 8AS-0011)

We appreciate the work done by your staff in examining certification and compliance reporting of DoD information technology systems. The reporting disparities identified by your staff point to the need for explanations in defining reporting requirements. They also point out inaccuracies in reports to OSD from the DoD Components.

We concur with each of your recommendations. We are in the process of updating the DoD Year 2000 Management Plan. We need your review of the update to make sure it improves guidance on verification and validation requirements, especially with regard to independent certification rather than self-certification. We also must update our reporting requirements quarterly, since the Office of Management and Budget modifies their request with each successive report. We will use the results of your audit to improve the reporting instructions. In addition, we will propose actions by the Deputy Secretary of Defense to make clear the importance of Year 2000 compliance and the enforcement of reporting and evaluation requirements.

We look forward to using the results of this and other audits to make sure DoD's Year 2000 efforts are successful.

Should you have any questions, please contact Ms. Sally Brown of the Year 2000 Oversight and Contingency Planning Office (703) 614-6934.

Arthur L. Money
Senior Civilian Official

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
Virginia G. Rogers
Jennifer L. Zucal
Frank C. Sonsini
Lusk F. Penn