~~FOR OFFICIAL USE ONLY~~

Audit Report

YEAR 2000 ISSUES OF A DEFENSE INFORMATION SYSTEMS AGENCY FIELD ACTIVITY

Report No. 99-175 June 2, 1999

Office of the Inspector General
Department of Defense

~~FOR OFFICIAL USE ONLY~~

Additional Information and Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup 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 Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

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

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C 20301-1900 The identity of each writer and caller is fully protected

Acronyms

C^4I	Command, Control, Communications, Computers, and Intelligence
DISA	Defense Information Systems Agency
JITC	Joint Interoperability Test Command
OMB	Office of Management and Budget
WHCA	White House Communications Agency
Y2K	Year 2000

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

June 2, 1999

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT. Audit Report on Year 2000 Issues of a Defense Information Systems Agency Field Activity (Report No 99-175)

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

DoD Directive 7650 3 requires that all recommendations be resolved promptly The Commander, White House Communications Agency, comments were partially responsive We request that additional comments be provided by August 9, 1999

Questions on the audit should be directed to [redacted] at (703) 604-[redacted] (DSN 664-[redacted]) ([redacted]@dodig osd mil) or [redacted] at (703) 604-[redacted] (DSN 664-[redacted]) ([redacted]@dodig osd mil) See Appendix B for the report distribution Audit team members are listed inside the back cover

[redacted]

Robert J Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-175 **June 2, 1999**
(Project No. 8AS-0032.18)

Year 2000 Issues of a Defense Information Systems Agency Field Activity

Executive Summary

Introduction. This report is one in 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. For a listing of audit projects addressing the issue, see the year 2000 webpage on the IGnet at http://www.ignet.gov.

Objectives. The overall objective was to evaluate the status of a Defense Information Systems Agency field activity, the White House Communications Agency (WHCA), in resolving its year 2000 computing issues.

Results. At the time of the audit, WHCA was considerably behind prescribed DoD and the Office of Management and Budget schedules for year 2000 conversion. However, WHCA has made an accelerated effort over the past months to complete testing and certification of its 78 systems. WHCA has identified 53 mission-critical and 23 mission-support systems. As of May 25, 1999, WHCA considered 67 of the 78 systems compliant, with 8 systems in the implementation phase. WHCA planned to complete testing and certification by the end of July 1999.

During the audit fieldwork that ended in February 1999, WHCA needed to identify interfaces and prepare written interface agreements; prepare and revise system and operational contingency plans; complete testing and prepare certification documentation; and report the status of all mission-critical systems to the DoD Year 2000 Office for inclusion in the DoD reporting to the Office of Management and Budget. We identified only three Year 2000 certification letters. See Finding section for details.

Summary of Recommendations. We recommend that the Commander, WHCA, identify external interfaces and prepare written interface agreements for WHCA managed mission-critical systems; finish preparing and revising system contingency plans; and officially move tested systems into the implementation phase for status reporting purposes. We also recommend the Director, Defense Information Systems Agency, report all WHCA mission-critical systems to the DoD Year 2000 Office to consolidate and include the data on those systems in the DoD reporting to the Office of Management and Budget.

Management Comments. The Commander, WHCA, concurred with the recommendations. In response to those recommendations, WHCA identified three mission-critical systems requiring bilateral interface agreements; planned to complete and validate operational contingency plans by June 1999; and reviewed and

improved test reporting and documentation. The Director, Defense Information Systems Agency, concurred with the recommendation on reporting all mission-critical systems to the DoD Year 2000 Office and stated that WHCA would continue to provide the Year 2000 database to the Defense Information Systems Agency Chief Information Officer, the J38 (NMCC) and the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). Subsequently, the DoD Year 2000 Steering Group affirmed that DoD will report the status of WHCA systems in future reports to the Office of Management and Budget. A discussion of management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Audit Response. We consider the management comments partially responsive. We request that the Commander, WHCA, provide additional comments on the status of written interface agreements and provide Year 2000 compliant certification letters for all mission-critical systems not previously provided by August 9, 1999.

Table of Contents

Background

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. The Executive Order establishes a policy that Federal agencies ensure that no critical Federal program experiences disruption because of the year 2000 (Y2K) problem. The head of each agency must ensure that efforts to address the Y2K problem receive the highest priority attention in the agency.

DoD Y2K Management Strategy. The DoD strategy for achieving Y2K conversion is set forth in the DoD Year 2000 Management Plan,* the latest version of which is dated December 1998.

White House Communications Agency Mission. The White House Communications Agency (WHCA) is an activity under the cognizance of the Defense Information Systems Agency (DISA). The mission of WHCA is to provide telecommunications and related support to the President, the Vice President, the President's staff, the Secret Service, and others as directed. Support provided by WHCA includes secure and nonsecure voice and data communications, printed message communications, audiovisual services, and photographic and graphics services both in the Washington, D.C., area and on a worldwide basis when the President, Vice-President, and First Family travel. WHCA also provides general purpose automated data processing for the National Security Council and the White House Military Office.

Role of the Defense Information Systems Agency. DISA is responsible for planning, developing, and supporting command, control, communications, and information systems for use in peace and war. DoD Directive 5105.19, "Defense Information Systems Agency (DISA)," June 25, 1991, tasks DISA with providing administrative support to WHCA. Administrative support includes budgeting, funding, and contracting support; legal counsel; and personnel management.

Joint Interoperability Test Command. The Joint Interoperability Test Command (JITC) is a DISA activity that supports the warfighters in their efforts to manage information on and off the battlefield. The support includes the following:

- conducting independent operational test, evaluation, and assessment of DISA and other DoD command, control, communications, computers, and intelligence (C^4I) acquisitions;
- identifying and solving C^4I and Combat Support Systems interoperability deficiencies;
- providing C^4I joint and combined interoperability testing, evaluation, and certification;

* Hereafter referred to as the DoD Y2K Plan.

- bringing C^4I interoperability support, operational field assessments, and technical assistance to the Commanders in Chief, Services, and agencies; and
- providing training on C^4I systems, as appropriate.

Objectives

The overall audit objective was to evaluate the status of the progress of WHCA in resolving its Y2K computing issues. See Appendix A for a discussion of the audit scope and methodology, our review of the management control program, and a summary of prior audit coverage related to the audit objectives.

Status of the White House Communications Agency Year 2000 Program

At the time of the audit, WHCA was considerably behind prescribed DoD and the Office of Management and Budget (OMB) schedules for Y2K conversion. WHCA needed to improve its Y2K program to minimize the risk of adverse impact of Y2K date processing problems on its mission and its mission-critical systems. More needed to be done in the following areas:

- complete the identification of interfaces and prepare written interface agreements for mission-critical systems with external interfaces;
- continue to prepare and revise system and operational contingency plans to establish alternate procedures to accomplish the WHCA mission;
- complete testing and prepare certification documentation to officially move tested systems into the implementation phase; and
- report the status of all mission-critical systems to the DoD Year 2000 Office so WHCA data can be consolidated and included in the DoD reporting to the OMB.

Although all risk cannot be eliminated, these actions would help minimize the risk of significant mission impairment. As of May 1999, WHCA reported accelerated progress to the Deputy Secretary of Defense.

Responsibilities for Addressing the Year 2000 Problem

The Chief Information Officer, DISA, has the principal responsibility of overseeing the Y2K effort for WHCA. WHCA established an internal Y2K Task Force to act as a conduit between the Y2K Program Manager and the operational directorates. The Y2K managers in each directorate are members of the task force and answer directly to the Y2K Program Manager. Although the task force had been working since the assessment phase, it had no formal mission or charter. The task force members are responsible for ensuring that the system points of contact take actions such as providing workbook documents, scheduling testing, and developing contingency plans.

As an operational test and evaluation asset of DISA, JITC was to conduct independent tests of the WHCA mission-critical systems. The primary tasking was to assist in the renovation, testing, validation, and implementation of Y2K solutions for each system. The statement of work required JITC to provide a full range of

services that included, but were not limited to, the following: hardware and software analysis, solution testing and documentation, contingency planning, and training.

JITC provides WHCA with monthly progress reports, develops test reports that communicate the results of the Y2K testing, and recommends the system level of compliance.

Identification of Systems

WHCA did not successfully complete its inventory and assessment of its mission-critical systems by the DoD target date of June 30, 1997. In August 1998, WHCA identified 68 mission-critical systems. The systems were broken down into the following categories: audio/visual, facilities and transportation, information systems, integrated mobile platforms, line of sight, radio systems, satellite systems, switching systems, and other. In November 1998, WHCA assigned a new Y2K Program Manager. Upon taking over the position, the new WHCA Y2K Program Manager made a reassessment of the mission-critical systems. He reduced the number of mission-critical systems from 68 to 52 systems. The reassessment reclassified systems as mission support, combined systems with other systems for testing, deleted systems, and added new mission-critical systems. On January 13, 1999, WHCA briefed DISA on the current status of its Y2K conversion program. The briefing described a reassessment of mission-critical systems. The briefing also indicated that 39 of the 52 mission-critical systems were noncompliant, and 13 were considered compliant. However, upon review of the documentation, we identified only three Y2K certification letters.

The original WHCA Y2K conversion strategy was to first process systems requiring the least extensive efforts. That would enable WHCA to move systems through the conversion process and into the implementation phase as quickly as possible to focus its attention on the systems requiring more extensive work. The WHCA Y2K conversion strategy appeared to be the most practical approach; however, WHCA did not fully implement the strategy.

WHCA did not prioritize the systems as required by the DoD Y2K Plan, which states, "Components must prioritize their mission-critical systems to determine which systems should be remedied first. . . . This prioritization must be done to determine the relative merits of fixing one system at the cost of not fixing another, in case enough resources or skilled personnel are not available to fix all systems in time." Prioritization would have helped to determine which mission-critical systems would require the most extensive conversion effort. In addition, prioritization would have helped to determine the interface requirements of the various systems and the impact that would result if those systems were not made Y2K compliant. Because WHCA is beyond the stage in which it needed to prioritize its systems, this report makes no recommendations to prioritize the systems.

Written Interface Agreements

WHCA did not prepare appropriate written interface agreements. WHCA manages mission-critical systems that interface with systems that other organizations managed both inside and outside of the Government. In reviewing the documentation for the various WHCA mission-critical systems, we found no interface agreements as required by the DoD Y2K Plan, Appendix F. The DoD Y2K Plan identifies interfaces that exchange format or protocol as critical because they have the potential to introduce or propagate errors from one organization to another. The DoD Y2K Plan states that, "Data trading partners can mitigate potential problems by agreeing on formats and schedules and by providing one another with test files."

We discussed the situation with the WHCA Y2K Program Manager. He indicated that the planned approach would be to issue letters of assurance to the activities that have interfaces to avoid what he termed the legal implications of a memorandum of agreement.

WHCA and their interface partners should discuss and verify that they have implemented consistent Y2K corrections for data passed between their systems. WHCA needs to prepare written interface agreements to reduce the risk of discovering too late in the Y2K effort that an interfacing system will not be able to accommodate the agency's own Y2K changes.

Contingency Plans

Importance of Contingency Planning. Contingency planning is an important element of applying risk management to the Y2K conversion effort. Contingency plans assist in providing insurance against Y2K disruptions by ensuring that plans exist to restore the system and to continue operations while normal system functions are not available. According to the DoD Y2K Plan, two primary types of contingency plans exist, system contingency plans and operational contingency plans. The operational contingency plan, also known as the operational continuity plan, addresses how an organization will continue to complete its mission or function in a "worst case" scenario. The DoD Y2K Plan prescribed that the mission-critical system contingency plans were to have been completed no later than December 31, 1998. Operational contingency plans were required by March 31, 1999. By June 30, 1999, all plans are to be exercised to determine their viability. In addition, the DoD Y2K Plan states that preparing contingency plans in accordance with the system prioritization level would help to focus planning efforts.

WHCA Contingency Plans. We reviewed the contingency plans for the mission-critical systems. We determined that WHCA did not develop contingency plans for each system, and those that it completed appeared inadequate. The contingency plans were inconsistent in their preparation and

varied greatly in their level of detail. The contingency plans did not always address the various aspects of the Office of the Assistant Secretary of Defense (Y2K) Contingency Plan Review in the DoD Y2K Plan, Appendix H. For example, the contingency plans lacked sufficient background information on the system and its interfaces; did not identify risks and contingencies; and did not discuss alternatives and the required resources to implement alternatives.

We briefed those concerns to the WHCA Y2K Program Manager, who subsequently decided to have all contingency plans rewritten.

WHCA Operational Contingency Planning. WHCA officials informed us that information on the operational contingencies was contained in a classified White House Military Office document. Because of the sensitivity of the information, we requested an unclassified description of the document. We made that request on numerous occasions throughout the audit field work. On all occasions, WHCA said that it would provide a statement. However, at the end of audit fieldwork, we were informed that WHCA could not provide us a statement and we should contact the White House Military Office directly. We contacted the White House Military Office, but because of classification issues, we were unable to review the document. Because we were unable to review the document, we could not verify the existence of a comprehensive contingency plan that covers the WHCA mission as required by the DoD Y2K Plan.

Testing and Compliance Checklists

According to the DoD Y2K Plan minimum exit criteria for the validation phase, WHCA had appropriately tested and documented only three mission-critical systems as Y2K compliant. As of February 18, 1999, WHCA had completed testing for 39 of its 52 mission-critical systems. WHCA reported that 35 of the 39 systems that it tested met the exit criteria for placement into the implementation phase. However, WHCA made the determination without identifying all interfaces for those systems, without adequate contingency plans, and without completing compliance checklists for system certification. Further, WHCA may have inappropriately reported systems to DISA as implemented and, therefore, compliant. A signed compliance checklist or acceptable equivalent did not support the classification of most of the systems identified as implemented. WHCA should not move systems from validation until the systems are fully tested and certified.

Testing. The DoD Y2K Plan prescribed that all mission-critical systems be tested and certified for Y2K compliance by September 30, 1998. Further, it states that the renovated and replacement systems should have been fully deployed by December 31, 1998. The OMB deadline for implementation of compliant, mission-critical systems was March 31, 1999. As of February 1999, WHCA had completed testing on approximately 75 percent, 39 of the 52 mission-critical systems. According to the WHCA Y2K Program Manager and supporting documentation, WHCA would not complete testing of 100 percent of the mission-critical systems until June 1999.

WHCA personnel stated that they were participating in one operational evaluation scheduled for March 1999, and that other interoperability and end-to-end testing would continue through the August and September timeframe.

Compliance Checklists. The DoD Y2K Plan, Appendix G, recommends the use of the Year 2000 Compliance Checklist to "aid system managers in ensuring that their systems are compliant for the year 2000." The plan provides an example of a checklist that contains items to be included in the Y2K testing and compliance process. The checklist helps to determine a system's overall Y2K compliance. The checklist provides a means of assuring system owners that their systems are certified and properly documented before considering them compliant.

Although WHCA personnel received the checklists, the application of the checklists was not consistent for all of the mission-critical systems. Appropriate use of the checklist would provide the information that would allow an analysis of the system's Y2K compliance.

Reporting Requirements

The DoD Y2K Plan states that mission-critical systems are to be reported and tracked in the DoD Y2K database and reported to OMB. Because of the nature of the WHCA mission, DISA decided to exclude the WHCA mission-critical systems from the database reporting process. Therefore, information regarding the Y2K conversion status of WHCA mission-critical systems was excluded from the DoD Y2K status report to OMB. WHCA stated that it reported its nuclear command and control systems to the Communications and Command and Control Battle Management Office of the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), that tracked the systems.

DISA should report the status of all WHCA mission-critical systems, in a declassified extract if necessary, to the DoD Year 2000 Office so the WHCA data can be consolidated and included in the DoD reporting to OMB.

Conclusion

DoD regards mission-critical systems that were not implemented by December 31, 1998, as high risk. Those that did not meet the OMB deadline of March 31, 1999, are considered as high risk by OMB as well. The status of all WHCA mission-critical systems needs to be reflected in the DoD Y2K data base and reported to OMB.

At the time of the audit, WHCA was considerably behind both DoD and OMB schedules for Y2K conversion. Although additional work is required, WHCA is catching up. On May 25, 1999, the Commander, WHCA, briefed the DoD Y2K Steering Committee. The Commander stated 67 of the 78 systems were

considered compliant and 8 systems had been moved into the implementation phase. Of the 67 compliant systems, 43 were mission-critical. Seven of the eight systems in the implementation phase were mission-critical. The Commander also stated that testing and certification of all systems would be completed by the end of July 1999.

Recommendations

1. We recommend that the Commander, White House Communications Agency:

a. Identify external interfaces and prepare written interface agreements for mission-critical systems that the White House Communications Agency manages.

b. Complete preparation and revision of mission-critical system contingency plans.

c. Finalize testing, prepare certification documentation and officially move systems into the implementation phase only after successfully testing and certification.

2. We recommend that the Director, Defense Information Systems Agency, report the status of all White House Communications Agency mission-critical systems, in a declassified extract if necessary, to the DoD Year 2000 Office so DoD can consolidate the data and include them in the DoD reporting to the Office of Management and Budget.

Management Comments

White House Communications Agency. The Commander, White House Communications Agency, concurred with Recommendations 1.a., 1.b., and 1.c. In response to those recommendations, the White House Communications Agency identified three mission-critical systems requiring bilateral interface agreements; planned to complete and validate operational contingency plans by June 1999; and reviewed and improved test reporting and documentation.

Defense Information Systems Agency. The White House Communications Agency coordinated with the Director, Defense Information Systems Agency, on Recommendation 2 and concurred. The Director, Defense Information Systems Agency, concurred with the recommendation and stated that the White House Communications Agency would continue to provide the Year 2000 database to the Defense Information Systems Agency Chief Information Officer, the J38 (NMCC) and the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

Audit Response

White House Communications Agency. Management comments were partially responsive. Management comments on Recommendation 1.a. stated that three White House Communications Agency systems have protocol interfaces with other organizations and require bilateral interface agreements. However, additional comments concerning the status of the written interface agreements and completion dates are requested. Management comments concerning Recommendation 1.b. were considered responsive and no further comments are requested. Management comments on Recommendation 1.c. stated documentation had been reviewed and improvements made. We request that the Commander, White House Communications Agency, provide us with Year 2000 compliant certification letters for all mission-critical systems not previously provided.

Defense Information Systems Agency. Management comments were responsive, especially in light of the clarification given at the May 25, 1999, DoD Y2K Steering Committee meeting at which it was decided that the status of all WHCA systems would be reported to the Office of Management and Budget.

Appendix A. Audit Process

Scope

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 Y2K computing challenge. For a listing of audit projects addressing the issue, see the Y2K web page on the IGnet at http://www.ignet.gov.

We reviewed and evaluated the status of the progress of WHCA in resolving the Y2K computing issue. Specifically, we evaluated the WHCA Y2K efforts against those required by the DoD Y2K Plan, which the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued in December 1998. We obtained a list of the mission-critical systems and reviewed documentation to include contingency plans, test plans, test reports, and external interface documentation. We reviewed WHCA documents dated from July 20, 1998, through May 25, 1999.

Scope Limitations. WHCA did not give us access to Special Mission Y2K system information. This prohibited us from reviewing information on two mission-critical systems. Although the Inspector General Act of 1978, as amended, specifies that only the Secretary of Defense can deny the Inspector General, DoD, access to records, we determined that coverage of the other WHCA systems provided sufficient basis for the audit finding on systemic issues in the WHCA Y2K conversion program.

DoD-Wide Corporate-Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, DoD established six DoD-wide corporate-level performance objectives. This report pertains to achievement of the following objective and goal:

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

General Accounting Office High-Risk Area. The General Accounting Office 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 program audit from November 1998 through February 1999 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did not rely on computer-processed data or statistical sampling procedures to perform 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 recognized the Y2K issue as a material weakness in the FY 1998 Annual Statement of Assurance.

Prior Audit Coverage

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

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
    Principal Director for Year 2000
Director, Defense Logistics Studies Information Exchange

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Information Systems Agency
  Commander, White House Communications Agency
  Inspector General, Defense Information Systems Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations and Individuals

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

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

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

Defense Information Systems Agency Comments

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

IN REPLY REFER TO: Inspector General (IG) 05 May 1999

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
(ATTN: ACQUISITION MANAGEMENT DIRECTORATE)

SUBJECT: Response to DoD IG Draft Report, Year 2000 Issues of a Defense Information Systems Agency Field Activity (Project 8AS-0032.18)

1. The following is the White House Communications Agency's (WHCA) response to the subject report:

Recommendation #1A: ...Commander, WHCA, identify external interfaces and prepare written interface agreements for WHCA managed mission-critical systems that WHCA manages.

Response: CONCUR. WHCA Systems fall into three categories:

1) Systems provided by other organizations to WHCA.
-WHCA obtains letter certifying compliance.
2) Systems provided by WHCA to other organizations.
-WHCA provides letters certifying compliance.
3) Systems that have protocol interfaces with other organizations.
-WHCA negotiates bilateral interface agreements.
(Only 3 WHCA systems are in this category)

Interfaces will be tested during End-to-End testing in July 1999.

Recommendation 1B: ...Commander, WHCA, complete preparation and revision of mission-critical system contingency plans.

Response: CONCUR. The Y2K program manager has completed contingency planning briefings to WHCA Directors and Division Chiefs. A standard DoD format was adopted to ensure critical information is provided including system interfaces. Updated system level plans will be completed, validated, and posted to the database by 15 May 99. Operational contingency plans will be completed and validated by June 1999. Operation contingency

Quality Information for a Strong Defense

plans will be subjected to Table-Top exercises during our July 1999 End-to-End testing.

Recommendation 1C: ... Commander, WHCA, finalize testing, prepare certification documentation and officially move systems into the implementation phase only after successfully testing and certification.

Response: CONCUR. Reporting and final documentation has been reviewed and improvements made. To date JITC has tested 73 of the 78 systems. 50 final test reports have been received for certification and review by WHCA. The remaining 23 draft reports have identified no Operational Y2K issues. The remaining 5 systems are being upgraded under contract and are subject to JITC Y2K validation as part of contract Test and Acceptance (TA) phase. Certification letters will be completed in May for those systems with final JITC test reports.

2. WHCA coordinated with DISA on recommendation 2 and the response is as follows:

Recommendation 2: ...Recommend that DISA report all WHCA mission-critical systems, in a declassified extract if necessary, to the DoD Year 2000 Office to consolidate the data and include them in the DoD reporting to the Office of Management and Budget.

Response: CONCUR. WHCA will continue to provide the Y2K database to the DISA CIO, J38(NMCC), and OSD C3I. This distribution will ensure DoD elements that WHCA interfaces with have pertinent Y2K information. DISA can forward Y2K information to other agencies as required.

3. If you have any questions, please call (b) (6)
Audit Liaison, at (b) (6)

(b) (6)

RICHARD T. RACE
Inspector General

White House Communications Agency Comments

INTEROFFICE MEMORANDUM

PMD - 990097

TO: Inspector General (IG)

FROM: Commander, White House Communications Agency (WHCA)

DATE: 3 May 99

SUBJECT: DoD IG Draft Report, Year 2000 Issues of a Defense Information Systems Agency Field Activity (Project BAS-0032.18)

Preparer: (b) (6)

1. Attached is the WHCA response to the subject report.

2. The subject report recommends DISA report the status of all WHCA mission critical systems to the DoD Y2K Office. WHCA will continue to provide the Y2K database to DISA CIO, J38 (NMCC) and OSD C31. This distribution will ensure DOD elements that WHCA interfaces with have pertinent Y2K information. DISA can forward Y2K information to other agencies as required.

(b) (6)

1 Incl.
as

Commanding

Copy to:
DISA CIO (ATTN: (b) (6)

Executive Summary

The Office of the Inspector General, DoD conducted an audit of the White House Communications Agency (WHCA) involving WHCA Y2K problem management and the resolution of Y2K computing issues The auditors cited several management issues and specific documentation shortfalls as weaknesses in the Y2K posture.

Much of the concern raised in the IG report revolves around WHCA attaining Y2K compliance for mission critical and mission support systems within the timeline established by DoD.

RECOMMENDATION 1A: INTERFACE AGREEMENTS.

Concur.

WHCA systems fall into 3 categories:

1) Systems provided by other organizations to WHCA.
   - WHCA obtains letter certifying compliance.
2) Systems provided by WHCA to other organizations.
   - WHCA provides letters certifying compliance.
3) Systems that have protocol interfaces with other organizations.
   - WHCA negotiates bilateral interface agreements.
     (only 3 WHCA systems are in this category)

Interfaces will be tested during End-to-End testing in July 1999.

RECOMMENDATION 1B: CONTINGENCY PLANNING.

Concur.

The Y2K program manager has completed contingency planning briefings to WHCA Directors and Division Chiefs A standard DOD format was adopted to ensure critical information is provided including system interfaces. Updated system level plans will be completed, validated and posted to the database by 15 May 1999. Operational contingency plans will be completed and validated in June 1999. Operational contingency plans will be subjected to Table-Top exercises during our July 1999 End-to-End testing.

RECOMMENDATION 1C: TESTING AND CERTIFICATION.

Concur.

Reporting and final documentation has been reviewed and improvements made. To date JITC has tested 73 of the 78 systems 50 final test reports have been received for certification and review by WHCA. The remaining 23 draft reports have identified no Operational Y2K issues The remaining 5 systems are being upgraded under contract and are subject to JITC Y2K validation as part of contract Test and Acceptance (TA) phase. Certification letters will be completed in May for those systems with final JITC test reports.

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.