Audit Report

DOD YEAR 2000 CONTINGENCY PLANS

Report No. D-2000-049 December 10, 1999

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 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 Future 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

COOP	Continuity of Operations Plan
GAO	General Accounting Office
OMB	Office of Management and Budget
Y2K	Year 2000

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

December 10, 1999

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

SUBJECT: Audit Report on DoD Year 2000 Contingency Plans (Report No. D-2000-049)

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

The Air Force Communications and Information Center comments conformed to the requirements of DoD Directive 7650.3; therefore, additional comments are not required. Therefore, we are publishing this report in final form.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. John J. Jenkins at (703) 604-9088 (DSN 664-9088) (jjenkins@dodig.osd.mil) or Mr. Scott S. Brittingham at (703) 604-9068 (DSN 664-9068) (sbrittingha@dodig.osd.mil). See Appendix B for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2000-049 **December 10, 1999**
(Project No. 9AS-0050)

DoD Year 2000 Contingency Plans

Executive Summary

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

Objectives. The overall objective was to determine whether contingency plans have been tested in accordance with the DoD Year 2000 Management Plan.

Background. The United States General Accounting Office, Office of Management and Budget, and the Office of the Assistant Secretary of Defense (Command, Control Communications, and Intelligence) have issued guidance stressing the importance of year 2000 contingency plans and Day One Guidance. Day One plans comprise a comprehensive set of actions to be executed by a federal agency during the last days of 1999 and the first days of 2000. The DoD Year 2000 Management Plan requires realistic contingency plans for all DoD mission-critical systems, and suggests the preparation of plans for all mission-essential systems.* Further, it requires that these system specific contingency plans map to broader operational contingency plans designed for activation in the event of broader functional failures. Contingency plans provide a means to minimize the adverse affects of year 2000 disruptions. They provide insurance against many possible types of year 2000 disruptions, ensuring that plans are in place to expedite the restoration of the system and to continue the mission or function while system support is not available, regardless of the reason for the disruption.

Results. Recent audit work continued to find mixed results in the quality of DoD contingency planning at both the system and operational levels. For 18 systems that were covered in this supplemental review, 13 systems had system contingency plans and 8 systems were mapped to operational contingency plans. We are aware that a

---

* Mission-critical systems are needed to ensure core national security mission capability. They receive priority for Y2K repair, testing, certification, and replacement. Mission-essential systems are those systems that while, not mission critical, are sufficiently important to smooth day-to-day operations to warrant Y2K compliance tracking. The loss of mission-essential functional or tangible capabilities and assets will have an adverse impact on the overall mission's functionality. Mission-essential systems are reported into the DoD Y2K Database as nonmission critical. No other nonmission-critical systems are reported.

number of DoD Components, to include the OSD Y2K Office, the Assistant Secretary of Defense (Health Affairs), the Department of the Air Force, and the Commander-in-Chief, U.S. Space Command, have recently reemphasized the need for adequate contingency procedures. No additional recommendations are made in this report.

Management Comments. Although no comments were required, the Air Force Communications and Information Center stated that they concurred with the general findings of the report. In addition, they stated that Air Force commanders will act on the concerns we documented, and as they wrap up their reviews of Y2K Continuity of Operations Plans, they are immediately correcting any deficiencies identified.

Table of Contents

Executive Summary i

Introduction

Background 1
Objectives 4

Finding

Contingency Planning Efforts 5

Appendixes

A. Audit Process
Scope 12
Methodology 13
Management Control Program 13
Summary of Prior Coverage 13
B. Report Distribution 14

Management Comments

Department of the Air Force Comments 19

Background

General Accounting Office Guidance. The General Accounting Office (GAO) issued the "Year 2000 Computing Crisis: Business Continuity and Contingency Planning" publication in August 1998. It was intended to aid in reducing the risk of year 2000 (Y2K) related failures. The GAO publication states that each plan should provide a description of the resources, staff roles, procedures, and timetables needed for its implementation. There are several key processes essential to contingency plan development, including:

- Assess benefits, costs, and risks of alternative contingency strategies.
- Select a strategy that is practical, cost effective, and appropriate to the organization.
- Develop a contingency plan that includes strategies capable of meeting minimum, acceptable output requirements for each business process.
- Define and document triggers for activating the contingency plans.
- Establish a business reputation team for each core business process.
- Develop and document "zero day" strategy and procedures.

The "Year 2000 Computing Crisis: Business Continuity and Contingency Planning" guide states that the objective of business continuity validation is to evaluate whether individual contingency plans are capable of supporting the core business processes. Validation should address: validation objectives, validation approach, required equipment and resources, necessary personnel, schedules and locations, validation procedures, expected results, and exit criteria. Validation should establish teams responsible for preparing and executing the contingency plans. Validation indicates that the plan adequately supports a core business function; is adequate to manage, record, and track the contingency processes; and the manual activities meet an acceptable level of performance. Plans should be updated based on validation lessons learned and should be revalidated if necessary.

Office of Management and Budget Reporting Requirements. On August 6, 1999, the Office of Management and Budget (OMB) issued memorandum number M-99-21 to the heads of selected agencies. The memorandum, titled "Revised Reporting Guidance on Year 2000 Efforts," created a new Y2K monthly requirement on the status of unfinished mission-critical systems and revised the quarterly reporting requirements. The memorandum required information on the progress in developing and testing the business continuity and contingency plans. In addition, OMB asked for information on how agencies were coordinating business continuity and contingency plans with their continuity of operations plans.

Year 2000 Management Plan. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued the most recent DoD Y2K Management Plan, Version 2.1, (DoD Y2K Management Plan) in September 1999. The DoD Y2K Management Plan states that systems, even compliant systems, may experience various degrees of disruptions as a result of problems with interfaces, user defined data, or the infrastructure. Systems that have been renovated and tested could fail, and the failure of one system could disrupt many others. Even more likely is that infrastructure disruptions could prevent the system from performing, even if the system itself is capable of correctly processing all data.

To ensure the continuation of all critical DoD functions into the next millennium, the DoD Y2K Management Plan requires realistic contingency plans for all DoD mission-critical systems, and suggests the preparation of plans for all mission-essential systems.* Further, it requires that these system specific contingency plans map to broader operational contingency plans designed for activation in the event of broader functional failures.

Contingency plans provide a means to minimize the adverse effects of Y2K disruptions. They provide insurance against the many possible types of Y2K disruptions, ensuring that plans are in place to expedite the restoration of the system and to continue the mission or function while system support is not available. Components are expected to review their contingency plans and those of their subordinate commands to ensure that all operational objectives will be met, the primary mission will be conducted, and that essential products or services will be delivered.

Y2K Operational Contingency Plan. According to the DoD Y2K Management Plan, operational contingency plans should identify alternative systems or procedures (workarounds) to use in the event a primary system is disrupted. Each core mission/function and critical process should have an operational contingency plan. The responsibility of developing and executing the operational contingency plans lies on the group responsible for executing the core mission process. Commanding Officers and civilian directors should document alternative systems able to sustain the minimum operational capabilities required in supporting the national military strategy. DoD Directive 3020.26 requires echelon II and above commands to develop Continuity of Operations Plans (COOP) to ensure the continuity of mission-critical operations during a national emergency. The DoD Y2K Management plan does not require the development of COOPs. However, if a COOP has been developed, it may be used in lieu of a Y2K operational contingency plan. The COOP must be

* Mission-critical systems are needed to ensure core national security mission capability. They receive priority for Y2K repair, testing, certification, and replacement. Mission-essential systems are those systems that while, not mission critical, are sufficiently important to smooth day-to-day operations to warrant Y2K compliance tracking. The loss of mission-essential functional or tangible capabilities and assets will have an adverse impact on the overall mission's functionality. Mission-essential systems are reported into the DoD Y2K Database as nonmission critical. No other nonmission-critical systems are reported.

made "Y2K aware" by updating its content, adding a Y2K appendix, and developing a strategy that addresses potential disruptions caused by Y2K.

Y2K System Contingency Plan. System contingency plans address activities to be performed by the system administrator, work group manager, or local area network manager, to preserve the system and its data. Plans should include technical workarounds necessary to recover the system, or use other system capabilities to sustain critical capabilities. The DoD Y2K Management Plan requires Y2K system contingency plans for all mission-critical systems. The DoD plans should be validated to ensure that the potential actions are executable. Operating manuals, procedural guides, and other directives governing the use of operational systems that have not been updated to include Y2K contingencies, are not considered adequate. System contingency plans are to map to at least one operational contingency plan. This ensures that in the event that the system is disrupted, an alternative system or procedure is available to continue the mission areas until the disrupted system is restored.

Year 2000 Contingency Planning Deadlines and Requirements. The DoD Y2K Management Plan required DoD to complete its mission-critical system contingency plans by December 30, 1998. Operational contingency plans were to be completed March 31, 1999. To ensure viability, the DoD Y2K Management Plan states that by June 30, 1999, all plans should have been exercised. Contingency plans are required or suggested for other systems. In addition, the DoD Y2K Management Plan states that the development of contingency plans for nonmission-critical systems should be prioritized.

Year 2000 Contingency Plan Validation. To assess whether contingency plan alternatives are realistic and executable, the contingency plans must be validated. Contingency plans should also be reviewed and updated on a regular basis to accommodate any changes, such as new or adjusted personnel and contact telephone numbers or new information obtained based on the outcome of contingency plan assessments. Contingency plans are validated primarily through exercises structured to validate the information and procedures in the plan. Objectives of validation include:

- verifying contingent procedures are correct and executable,
- verifying information is correct and accurate,
- verifying that all personnel understand their roles involved, and
- identifying deficiencies in the plan.

The most common types of validation methods include tabletop exercises, procedure verification exercises, and actual operations exercises. Tabletop exercises are discussions of actions that will be taken. Procedure verification includes a review of contingency plan operations to verify support of the recovery strategy, and actual operations exercises involve shutting down the primary system and re-establishing the application at a back-up site. The actual operations exercises provide the greatest opportunity to conduct training and raise the level of assurance in the contingency plan.

Objectives

The overall objective of the audit was to determine whether contingency plans have been tested in accordance with the DoD Year 2000 Management Plan. See Appendix A for a discussion of the audit scope, methodology, and prior audit coverage.

Contingency Planning Efforts

Recent audit work continued to find mixed results in the quality of DoD contingency planning, at both the system and operational levels. For 18 systems that were covered in this supplemental review, 13 systems had system contingency plans and 8 systems were mapped to operational contingency plans. We are aware that a number of DoD Components, to include the OSD Y2K Office, the Assistant Secretary of Defense (Health Affairs), the Department of the Air Force, and the Commander-in-Chief, U.S. Space Command, have recently reemphasized the need for adequate contingency procedures.

Completed Inspector General, DoD Audit Work

We have issued three Y2K Summary Reports: Report No. 99-059, "Summary of Year 2000 Conversion -- Audit and Inspection Results," December 24, 1998; Report No. 99-115, "Summary of DoD Year 2000 Audit and Inspection Reports II," March 29, 1999; and Report No. 99-247, "Summary of DoD Year 2000 Audit and Inspection Reports III," September 3, 1999. In total, those three reports summarized 173 other reports that identified shortfalls in contingency planning efforts. Since the issuance of the third summary report on September 30, 1999, the Inspector General, DoD, has completed another 21 audits that have included reviews of contingency plans. Overall, these 194 audits have identified contingency planning shortfalls across virtually the entire spectrum of DoD organizational components. Additional ongoing Inspector General, DoD, audits have potential findings or observations related to contingency planning. Results from contingency plan reviews under this project are similar to findings in other previous and ongoing audits. These recent audit findings indicate that DoD needed to continue working to complete and validate its contingency plans.

Results from Contingency Plan Reviews Under this Project

Our review supplemented the work discussed above and focused on the Navy and the Air Force. We excluded the Army because it had already deviated from the DoD Management Plan, before our review began, and set September 30, 1999, as its own milestone for completing contingency plan validation. Other DoD Components were excluded because of ongoing coverage of their contingency planning by other Inspector General, DoD, auditors.

We observed three issues during our review. System owners did not: document contingency plan test results, update plans to reflect lessons learned after validation, or believe additional resources were required to execute the contingency procedures. Additionally, our review confirms that some DoD contingency plans lack stand-alone attributes that provide evidence that prescribed procedures are realistic and executable. Further, we believe the successful execution of Y2K contingency procedures remains overly dependent on the pre-existing knowledge of the DoD mission/function operators.

We initially selected five mission-critical systems and five mission-essential systems each from the Navy and the Air Force. During our review, we encountered five systems that were decommissioned and replaced by other systems, for which we requested the same information asked about the original system. In addition, the Navy decommissioned, without replacement, one of the mission-critical systems and the Air Force terminated one mission-essential system.

Overall, we reviewed eight mission-critical systems and ten mission-essential systems. One of the systems originally designated as mission-critical was replaced by a mission-essential system while one additional mission-critical and one mission-essential system was terminated. The system point of contact questioned the mission criticality of the original system and stated that the replacement system was not mission critical.

Questionnaire. We developed a Y2K contingency plans questionnaire to obtain general information on system and operational contingency planning. In addition to asking questions on the validation of the contingency plans, the questionnaire requested copies of the system contingency plan as well as the operational contingency plan to which the system plan maps. We also asked for a signed copy of the test plan and results of operational contingency plans that were tested.

Contingency Plans. System contingency plans detail the procedures necessary to restore a system in the face of all Y2K disruptions. Operational contingency plans detail the procedures for continuing the mission/function supported by the system(s) during any prolonged disruption.

Although the DoD Management Plan suggests, rather than requires, that mission-essential systems have contingency plans, it is advisable for every system and function to have contingency plans to help mitigate problems should Y2K disruptions occur. Some reasons include:

- Unclear definition of mission critical. Through various reviews, we have determined that organizations may not be certain whether or not to label their system mission critical, as the definitional boundaries are subjective.

- There are links between mission-critical and nonmission-critical systems. Therefore, Y2K disruptions in a mission-critical system may affect a nonmission-critical system, and vice versa.

- Failure of nonmission-critical systems may disrupt the mission-critical functions they support. Not having a contingency plan for the nonmission-critical systems could worsen the effects.

- Many nonmission-critical systems are defined as mission-essential, and, therefore, must be important to the function. Any Y2K disruptions to these systems may be detrimental to the function.

Operational Contingency Plans. For the 18 systems reviewed, system managers provided operational contingency plans for four of the eight mission-critical systems. One plan was called a programmatic contingency plan but included elements of an operational contingency plan. The other four system managers either did not have one or stated they did not have insight into which operational plan their system contingency plan mapped into. Four of the ten mission-essential systems mapped to operational contingency plans; the plans were provided to us. The remaining six mission-essential systems did not have an operational plan, and specifically, three system managers stated that they had no contingency plans. Although some results from our operational contingency plan review are included, the results listed are based mainly on the responses from the questionnaire.

Documentation of Contingency Test Results. Of the 18 systems we reviewed, 4 system managers stated they had operational contingency plan testing documentation. Three of the systems were mission critical and one was mission essential. The test results provided were of varied levels of detail.

Contingency Plan Updating. As part of our questionnaire, we asked whether or not the operational contingency plan validation/exercise resulted in updating the contingency plan. Only two system owners stated that they updated the operational contingency plan as a result. However, one system owner did not state what was updated or when revalidation would occur. The other system owner stated that the appendices were updated to incorporate new hardware and software releases. Both provided the scheduled revalidation date.

Additional Resources. The responses to our question about whether any additional resources were required to execute the contingency plans were mostly negative. Only one system owner stated that additional resources would be needed. The system owner stated that resources would only be necessary should the outage exceed 30 days, but had not determined the resource requirements. However, through review of the operational contingency plans, we found three additional plans that stated additional resources may be needed for execution. One plan estimated dollar amounts, however, did not itemize. The other two plans stated that additional manpower would be required. In addition to increased manpower, one stated contingency execution would require an increase in fuel load as well.

System Contingency Plans. We received copies of 13 system contingency plans for the 18 systems reviewed. All eight mission-critical systems had system contingency plans; two plans were labeled programmatic contingency plan but appeared to be system contingency plans. Three of the five mission-essential systems without system contingency plans also did not have an operational contingency plan. Although the DoD Year 2000 Management Plan does not require nonmission-critical systems to have contingency plans, it is advisable that every system should have one to help prevent any problems should Y2K problems disrupt operations. The results of our review are based on the answers to the questionnaire items related to system contingency plans and our review of the 13 system contingency plans we received.

Stand-alone attributes. Our review of the 13 system contingency plans showed that, overall, the contingency plans lacked the stand-alone attributes that provide evidence that prescribed procedures are realistic and executable. Some plans relied on boilerplate information to state that they will do something, rather than determining and developing alternative solutions and indicating how to implement those actions. For example, one system's procedures for operating in contingency mode included undertaking several actions simultaneously should the plan be invoked, including "Establish a help desk [Point Of Contact] that will continue to coordinate activities until the system has been corrected." and "Begin immediate corrective action to correct system deficiencies that led to the data corruption, and develop procedures for restoring the data integrity of the database." Another system contingency plan included a training plan which stated, the command "is responsible for ensuring operators are properly trained in manual requisition processing procedures." Neither of the plans discussed procedures for how to implement their contingency plans, they simply used the boilerplate information to state they will perform some task.

Pre-existing Knowledge. We determined that the successful execution of the contingency procedures is overly dependent on pre-existing knowledge of the DoD mission/function operators. Some of the plans reviewed stated what they planned as contingency operations, but not in a way that another individual could perform the tasks. For example, one system contingency plan stated as a preparatory action for hardware failure that they would "perform periodic data system and application software backups" and they should "ensure maintenance contracts are in place." These functions require pre-existing knowledge of the organization, system, and function. If an individual is expected to perform these duties as part of contingency operations, but does not have fairly extensive pre-existing knowledge of all the system and application software and data, including what maintenance contracts exist, the contingency plan will be of little use.

Continued Emphasis on Contingency and Day One Planning

Office of Management and Budget. Overall, the Government continues to place a high priority on contingency and Day One Planning. Day One Planning comprises a comprehensive set of actions to be executed during the last days of 1999 and the first days of 2000. Specifically, Day One Plans describe agency-planned activities during the pre-rollover and post-rollover periods. OMB recently issued Memorandum No. M00-01, "Day One Planning and Request for Updated Business Continuity and Contingency Plans," October 13, 1999. It states it is important to plan and prepare for the end of December and early January to help mitigate any problems. It also states that Day One Plans should address the full scope of agency activity that will be underway during that period, including efforts to mitigate the impact of possible failures in internal systems, buildings, and other infrastructure. In addition, the OMB has been requiring summary-level data on contingency plans for mission-critical systems as part of the agency quarterly reporting process on Y2K readiness.

General Accounting Office. GAO has issued Day One Planning guidance, "Y2K Computing Challenge: Day One Planning and Operations Guide," October 1999. The guidance states that a Day One strategy should be developed to address challenges created by the millennium turnover. It states that Day One Planning objectives are to:

- position an organization to readily identify Y2K induced problems, take needed corrective actions, and minimize adverse impact on agency operations and key business processes; and

- provide information about an organization's Y2K condition to executive management, business partners, and the public.

DoD Year 2000 Quarterly Progress Report. The DoD eleventh quarterly progress report on the status of Y2K efforts, dated November 15, 1999, states that the DoD mission-critical systems had system contingency plans in place and they were being rehearsed, refined, and reviewed by external and internal auditors. It stated that the Chairman of the Joint Chiefs of Staff conducted a series of contingency assessments to determine whether key warfighting tasks could be accomplished if key systems became unavailable. DoD conducted a series of table top exercises to prepare senior leaders for possible policy decisions that might be generated by Y2K problems.

The Chairman of the Joint Chiefs of Staff contingency assessments assessed the ability of DoD to respond with timely decisions in a Y2K degraded environment and focused on the strategic national tasks of mobilization, deployment, employment, intelligence-surveillance-reconnaissance, and sustainment. This series of exercises was designed to achieve senior management participation in and awareness of the operational impact of Y2K mission-critical systems failure during the mobilization, deployment, employment, and sustainment process. In addition, the exercises assessed the ability of the Services to execute operational contingency plans and to mitigate problems associated with Y2K.

The table top exercises were to enhance participants' understanding of potential Y2K impacts on national security; assist in the development of policy recommendations; provide continuing impetus to accelerate progress on fixing Y2K systems problems; and facilitate effective contingency planning.

DoD Testimony on Contingency Plans. On October 29, 1999, the Deputy Assistant Secretary of Defense, Deputy Chief Information Officer/Year 2000 testified to the House Science Subcommittee on Technology joint hearing with House Government Reform Subcommittee on Government Management, Information, and Technology on Y2K Day One Contingency Plans. During the testimony, he stated that the Chairman of the Joint Chiefs of Staff conducted a series of contingency assessments. The assessments evaluated the impact on military operations in the event of system loss and the support of the contingency plans that would be put in place should those systems be removed. "[DoD] also conducted business continuity planning in terms of both systems continuity plans and operational continuity plans, meaning that we have a continuity plan for every system, and we have a continuity plan for every

operational functional area that is a combination of systems or a larger function." Further, " . . . we have a way to support loss of capability in any one of those events."

Recent DoD Actions. The OSD Y2K Office, the Assistant Secretary of Defense (Health Affairs), the Department of the Air Force, and the Commander-in-Chief, U.S. Space Command have recently reemphasized the need for adequate contingency procedures. In October 1999, the OSD Y2K Office provided the DoD Components with a list of "Top Ten" concerns on contingency planning. The topmost concern was the executability of contingency plans. An October 27, 1999, Chief of the Staff, Air Force, message, "Homestretch to Year 2000," emphasized that contingency and continuity of operations plans had to be refined and reviewed to ensure that people knew how to use them and that additional resources needed to execute the plans had to be finalized. The Commander-in-Chief, U.S. Space Command, in his November 3, 1999, memorandum, "Year 2000 Consequence Management," noted that his review had identified many of the same "Top Ten" concerns listed by the OSD Y2K Office. He encouraged his command elements to renew efforts to ensure that they met Y2K contingency planning requirements and that their reviews specifically address the "Top Ten" list of contingency planning concerns. A November 7, 1999, Assistant Secretary of Defense (Health Affairs) memorandum, "Certification of Medical Department Year 2000 Preparations," required that each Service Medical Department certify its medical Y2K preparedness by December 20, 1999, and further stated that the certification shall attest to the operational readiness of day-one strategies. Additionally, in a November 19, 1999, electronic message to the DoD Component Y2K representatives, the Principal Director, Year 2000, stated that the validity and executability of contingency plans will continue to be an issue up to and after the day rollovers for the century and leap year. Further, he asked that the Components particularly review the contingency plans for trusted systems and systems not yet complete and that they use the "Top Ten" list of concerns in their reviews.

Conclusion

Inspector General, DoD, audit results indicate that managers and commanders at all levels must continue to focus on viable contingency procedures and adequate Day One Planning to minimize Y2K risks. Although time is running out for further system testing and various other risk mitigation measures, managers and commanders at all levels could profitably use the remainder of December 1999 to fine tune, test, and train personnel on contingency plans.

Management Comments

Although not required to comment, the Air Force Communications and Information Center stated that they concurred with the general findings of the report. In addition, they stated that Air Force commanders will act on the

concerns we documented, and as they wrap up their reviews of Y2K Continuity of Operations Plans, they are immediately correcting any deficiencies identified.

Appendix A. Audit Process

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 list of audit projects addressing the issue, see the Y2K web pages on IGnet at http://www.ignet.gov/.

Scope

Work Performed. We developed the Year 2000 Contingency Plan Questionnaire using requirements in the DoD Year 2000 Management Plan, September 1999, Version 2.1. We judgmentally selected 20 systems. We specifically looked at five mission-critical systems and five nonmission-critical systems from each of the Air Force and Navy. The selected systems were required to complete a questionnaire and to provide copies of the operational and system contingency plans. We evaluated the completeness of the questionnaire responses and the adequacy of the contingency plan, in accordance with the DoD Year 2000 Management Plan, September 1999, Version 2.1. We documented similarities and differences between the responses and what was found in the contingency plans.

DoD-wide Corporate Level Government Performance and Results Act Goals. In response to the Government Performance Results Act, the Department of Defense has established 2 DoD-wide objectives and 7 subordinate performance goals. This report pertains to achievement of the following goals (and subordinate performance goals):

- **DoD Corporate Level Goal 2:** Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure. **(00-DoD-2.0)**

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

- **Information Technology Management Functional Area. Objective:** Become a mission partner. **Goal:** Serve mission information users as customers. **(ITM-1.2)**

- **Information Technology Management Functional Area.**
  Objective: Provide services that satisfy customer needs.
  Goal: Modernize and integrate Defense information infrastructure. **(ITM-2.2)**

- **Information Technology Management Functional Area.**
  Objective: Provide services that satisfy customer needs.
  Goal: Upgrade technology base. **(ITM-2.3)**

General Accounting Office High-Risk Area. In its identification of risk areas, the General Accounting Office has specifically designated risk in the Y2K as high. This report provides coverage of that problem of the overall Information Management and Technology high-risk area.

Methodology

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from July 1999 through November 1999 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 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 1998 Annual Statement of Assurance.

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 at http://dodig.osd.mil.

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense for Policy
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)
  Deputy Assistant Secretary of Defense (Command, Control, Communications, and Intelligence, Surveillance, Reconnaissance, and Space Systems)
  Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
    Principal Director for Year 2000
Assistant Secretary of Defense (Force Management Policy)
Assistant Secretary of Defense (Health Affairs)
Assistant Secretary of Defense (International Security Affairs)
Assistant Secretary of Defense (Legislative Affairs)
Assistant Secretary of Defense (Nuclear and Chemical and Biological Defense Programs)
Assistant Secretary of Defense (Public Affairs)
Assistant Secretary of Defense (Reserve Affairs)
Assistant Secretary of Defense (Special Operations/Low Intensity Conflict)
Assistant Secretary of Defense (Strategy and Threat Requirements)
General Counsel of the Department of Defense
Director, Operational Test and Evaluation

Joint Staff

Director, Joint Staff

Department of the Army

Chief Information Officer, Army
Inspector General, Department of the Army
Auditor General, Department of the Army

Department of the Navy

Chief Information Officer, Navy
Naval Inspector General
Auditor General, Department of the Navy
Inspector General, Marine Corps
Superintendent, Naval Postgraduate School

Department of the Air Force

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

Unified Commands

Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Joint Forces 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

Other Defense Organizations (cont'd)

Director, Defense Finance and Accounting Service
  Chief Information Officer, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
  Chief Information Officer, Defense Logistics Agency
  Commander, Defense Contract Management Command
Director, Defense Security Cooperation Agency
Director, Defense Security Service
  Chief Information Officer, Defense Security Service
Director, Defense Threat Reduction Agency
  Chief Information Officer, Defense Threat Reduction Agency
  Inspector General, Defense Threat Reduction Agency
Director, National Imagery and Mapping Agency
  Inspector General, National Imagery and Mapping Agency
Director, National Security Agency
  Inspector General, National Security Agency
Director, Washington Headquarters Services
Inspector General, Defense Intelligence Agency
Inspector General, National Reconnaissance Office

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

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, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Committee on Science

Department Of Air Force Comments

DEPARTMENT OF THE AIRFORCE
HEADQUARTERS UNITED STATES AIR FORCE

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING
OFFICE OF THE INSPECTOR GENERAL
DEPARTMENT OF DEFENSE

FROM: HQ USAF/SC
1250 Air Force Pentagon
Washington DC 20330-1250

SUBJECT: DoDIG Draft Report, DoD Year 2000 Contingency Plans (Project No. 9AS-0050)

This is in reply to your memorandum distributed to the Assistant Secretary of the Air Force (Financial Management and Comptroller). We appreciate the important work you have accomplished in highlighting Year 2000 (Y2K) contingency planning and the opportunity to comment on our Y2K contingency planning efforts. We concur in principle with your general findings and are confident that Air Force commanders will act on the concerns you have documented.

The Air Force considers Y2K contingency planning of paramount importance for readiness. The Air Force has taken enormous steps to ensure plans are written and tested. We published an Air Force instruction that specifically requires commanders at all levels to develop Y2K contingency plans. We completed multiple audits within the service to ensure plans are complete and executable. We are wrapping up Y2K Continuity of Operations Plan (COOP) reviews with Air Force Audit Agency and Air Force Communications Agency Strike Teams in Europe this week. Any deficiencies identified are being corrected on the spot. All Air Force installation commanders have certified that COOPs have been written and exercised. Finally, the Chief of Staff of the Air Force sent out a message on 27 Oct 99 (attached) stressing the need to refine plans, train personnel on the use of those plans and nail down the resources to execute the plans. Although contingency planning is nothing new for the Air Force, these additional steps to ensure plans are written and tested is unprecedented.

Our system maintainers routinely respond to system anomalies and have good contingency plans in place. They do not always have visibility into their user's contingency plans should the systems that support them fail. Because there could be multiple reasons a system is unavailable (i.e. loss of network backbone, commercial communications or commercial power), the Air Force has stressed a mission-centric focus to contingency planning versus system-centric. Once we ascertain specific deficiencies in any contingency plans we will forward that information to the appropriate office for action.

Again thank you for your efforts. Please contact Maj William Hostetler, 602-2303, william.hostetler@pentagon.af.mil, should you have any questions.

WILLIAM J. DONAHUE, Lt Gen, USAF
Director, Communications and Information

Attachment:
CSAF Homestretch to Year 2000 (Y2K) Message
272156Z Oct 99

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report.

Thomas F. Gimble
Mary Lu Ugone
Kathryn M. Truex
Scott S. Brittingham
John J. Jenkins
William R. Pusey
Ericka P. Savage
Kevin W. Klein