Audit Report

YEAR 2000 CONVERSION PROGRAM AT
THE ARMY NATIONAL GUARD

Report No. 99-194 June 29, 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

ARNG	Army National Guard
Y2K	Year 2000

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

June 29, 1999

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
CHIEF OF STAFF, DEPARTMENT OF THE ARMY
CHIEF, NATIONAL GUARD BUREAU
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Year 2000 Conversion Program at the Army National Guard (Report No. 99-194)

We are providing this report for information and use

We considered comments from the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and the Chief, National Guard Bureau, to the draft report in preparing the final report. Accordingly, we deleted the recommendation to finding C and revised the finding itself. Management comments were responsive and conformed to the requirements of DoD Directive 7650.3; therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Raymond A. Spencer, at (703) 604-9071 (DSN 664-9071) (rspencer @dodig.osd.mil) or Mr. Michael E. Simpson at (703) 604-8972 (DSN 664-8972) (msimpson @dodig.osd.mil). See Appendix C for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-194 **June 29, 1999**
(Project No 9AB-0080.00)

Year 2000 Conversion Program at the Army National Guard

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 in addressing the Year 2000 computing problem. For a listing of audit projects addressing the issue, see the Year 2000 webpage on the IGnet at http://www.ignet.gov.

Objectives. The primary audit objective was to determine whether the Army National Guard was adequately preparing its information technology systems to resolve date-processing issues for the year 2000 computing problem. Specifically, the audit determined whether the Army National Guard had developed risk assessments, testing, and contingency plans.

Results. When we issued the draft report on April 16, 1999, 5 of the 11 Army National Guard mission-critical systems had not met the Office of Management and Budget's compliance deadline of March 31, 1999. However, four of the five systems were compliant by June 1999. The system contingency plans did not address continued operations of the Army National Guard. In addition, the Army National Guard did not have plans or a schedule for testing the contingency plans. The Army National Guard had made progress in ensuring that its Communications Operational Contingency Plan could be implemented if communications failed as a result of Y2K disruptions, but needed to do more work on other operational contingency planning.

Summary of Recommendations. We recommend that the Director, Army National Guard, update the system contingency plans to include resource requirements, degraded system functionality, impacts to hardware and software and detailed solutions and workarounds; prepare a schedule to complete the analysis of mission-critical functions and operational contingency plans; prepare test plans and schedules to test the plans in an exercise; assign a high ranking official at the Army National Guard to monitor and report the progress in establishing contingency plans and testing dates; and update the risk management plans.

Management Comments. The Director, Army National Guard, concurred with findings A and B and the related recommendations, but nonconcurred with finding C and the assessment of risk of failure of the Communications Operational Contingency Plan. Officials stated that recent test results demonstrated a high degree of success in the communications plan.

The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) supported the findings and recommendations. The Assistant Secretary also

stated that his office had reviewed and was satisfied with the Army National Guard progress in correcting the identified deficiencies, especially those pertaining to the operational contingency plans. He also noted that funding remained as a concern.

Audit Response The management comments were responsive. Based on those comments, we changed finding C to include recent test results and requirement changes, and deleted the recommendation pertaining to that finding.

Table of Contents

Executive Summary i

Introduction

Background 1
Objectives 2

Findings

A. Army National Guard Mission-Critical System Year 2000 Compliance 3
B. System Contingency Plans of the Army National Guard 5
C. Operational Contingency Plan for Communication 9

Appendixes

A. Audit Process
Scope 12
Methodology 13
Summary of Prior Coverage 13
B. Mission-Critical System Descriptions and Status 14
C. Report Distribution 16

Management Comments

Office of the Assistant Secretary of Defense (Command Control Communications and Intelligence) 19
Army National Guard 20

Background

The Year 2000. Information technology systems have typically used two digits to represent the year, such as "98" representing 1998, to conserve electronic data storage and reduce operating cost. With the two-digit format, however, the year 2000 is indistinguishable from 1900. As a result of the ambiguity, computers, associated systems, and application programs that use dates to calculate and sort could generate incorrect results when working with years after 1999.

Y2K Management Plans. The "DoD Year 2000 Management Plan," was first issued in April 1997 and was updated in January 1999. The DoD Y2K Management Plan provides the overall DoD strategy and guidance for inventorying, prioritizing, repairing or retiring systems, and monitoring progress. The "U.S. Army Year 2000 (Y2K) Action Plan" first issued in March 1996 and updated in June 1998, provides guidance and defines roles and responsibilities for addressing Army Y2K problem. The plan supports the DoD Y2K Management Plan.

Army National Guard. The Army National Guard (ARNG) consists of units in 2,700 communities in all States, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands. During peacetime, ARNG units are under the control of their respective State or Territory and provide support for emergency relief, search and rescue operations, civil defense, vital public services, and counter drug operations. The Federal mission of the ARNG is to maintain well-trained and well-equipped units available for prompt mobilization during war and to provide assistance during national emergencies. The ARNG identified 11 mission-critical systems that they use in performing their mission. The ARNG owns, operates, and is responsible for the Y2K compliance of the 11 mission-critical systems. See Appendix B for a listing and description of the systems.

ARNG State Headquarters Y2K Programs. We visited 10 ARNG State Headquarters to determine the status of the Y2K programs within the State. The State Headquarters visited were Alaska, California, Florida, Georgia, Idaho, Nevada, New Jersey, New Mexico, New York and Texas. All work on Y2K compliance started late because of little guidance from the ARNG; however, by January 1999, the States had begun to work the Y2K issues. Because most mission-critical systems used by the States belong to either the Army or the National Guard Bureau, the State ARNG Headquarters addressed only infrastructure systems within the State. All were in the assessment phase to determine the scope of Y2K problem, its effects on infrastructure systems, and action needed. The ARNG State Headquarters were also in contact with the utility providers within the State and were monitoring the utility providers' Y2K progress.

Emergency Response Plans. The plans of the 10 ARNG State Headquarters included standard operating procedures to provide military support to civilian authorities. Once the National Guard is activated by the State, it becomes a

State agency under the State Emergency Management Agency responsible for emergency response and recovery. The State Government Emergency Management Plan defines the standard operating procedures for State emergencies and establishes operational concepts, identifies tasks, and outlines policies, procedures and responsibilities for each State agency. All 10 States' Governments and the National Guard State Headquarters believed that the procedures worked well and will use them in a Y2K emergency. Additionally, States' and National Guard State Headquarters' personnel were determining Y2K risks and vulnerabilities and the effects or changes, if any, on their emergency response and recovery plans.

Objectives

The primary audit objective was to determine whether the ARNG was adequately preparing their information technology systems to resolve date-processing issues for the Y2K computing problem. Specifically, the audit determined whether the ARNG developed risk assessments, testing, and contingency plans. Appendix A describes audit scope and methodology.

A. Army National Guard Mission-Critical Systems Year 2000 Compliance

Five of 11 ARNG mission-critical systems did not meet the Office of Management and Budget's compliance deadline of March 31, 1999. However, four of the five systems were compliant by June 1999. Only the Retirement Points Accounting Management System remained noncompliant, with an estimated completion date of September 1999. Therefore, the ARNG made considerable progress in making its mission-critical systems complaint.

System Compliancy Requirements

The Office of Management and Budget required Federal agencies to have all mission-critical systems Y2K compliant by March 31, 1999. The DoD Y2K Management Plan makes DoD Components responsible for implementing the five-phase Y2K management process. The phases include awareness, assessment, renovation, validation and implementation. The DoD Y2K Management Plan also requires system developers to prepare documentation including test plans, test analysis reports, risk management plans, and system contingency plans to support the compliance process. Additionally, the system manager must certify and document each system's Y2K compliance.

Status of ARNG Mission-Critical Systems

The ARNG identified 11 mission-critical information systems. See Appendix B for a description of the 11 systems. The result of our review of the 11 systems follows.

Noncompliant Systems. Only one mission-critical system remained noncompliant as of June 1999. This system is the Retirement Points Accounting Management System, which has an estimated Y2K implementation date of September 1999.

Compliant Systems. Six mission-critical systems met the Office of Management and Budget's March 31, 1999, compliance deadline. These systems included the Automated Fund Control Order System, the Aviation Logistic Readiness Model, the Joint Uniform Military Pay Service Standard Terminal Input System, the Training Readiness Operations Unit Planning Execution Resourcing System, the User-Based ARNG System, and the State Accounting Budget Expenditure Reservation System. Four mission-critical systems were compliant after the March 31, 1999, date but before June 1999. These systems included the Standard Installation Division Personnel System, the Reserve Component Management System-Guard; the Total Army Personnel Database-ARNG, and the Manpower Voucher System.

Documentation

We reviewed program documentation for all 11 mission-critical systems. The ARNG prepared a schedule to show planned Y2K certification dates for the noncompliant systems. The ARNG was working to complete, or had completed, the required test plans, test analysis reports, risk management plans, and system contingency plans for the five noncompliant systems. All compliant systems had the required certification checklists, test plans, test analysis reports, risk management plans, and system contingency plans.

The test plans identified test processes and documentation required to support certification. The plans included material needed for testing and performance requirements, and scenarios for all functions with date-related calculations. In addition, the plans included interface tests to ensure proper formatting and processing with other systems and criteria to evaluate the test results. The test reports showed test results, Y2K issues, functional issues, effects on interfaces, recommendations, and conclusions. The risk management plans and the system contingency plans are discussed in finding B.

Conclusion

While 5 of the 11 ARNG mission-critical systems were noncompliant as of March 31, 1999, all but one system was compliant by June 1999. Therefore, because the ARNG was working to ensure that systems become Y2K compliant, we are making no recommendations.

Management Comments on the Finding

The Director, ARNG, concurred with the finding and stated that since the report was written, three of the five noncompliant systems had been certified. The systems include the Manpower Voucher System, the Reserve Component Management System-Guard, and the Total Army Personnel Database-ARNG system. The Director stated that the Standard Installation Division Personnel System would be certified by June 1999. Army officials verified that the system was compliant by May 1999, and they will certify the other system by September 1999. The Assistant Secretary of Defense (Command, Control Communications and Intelligence) fully supported the finding.

B. System Contingency Plans of the Army National Guard

The system contingency plans of the ARNG were not adequate to address continued operations and the ARNG had no operational contingency plans except for communications. In addition, the ARNG did not have plans or a schedule for testing the contingency plans. This condition occurred because of a lack of management priority on Y2K contingency planning and inadequate system risk management plans. As a result, the ARNG needed to do more to minimize the risk of adverse mission impact because of Y2K issues.

Risk Management and Contingency Planning Requirements

The "U.S. Army Year 2000 (Y2K) Action Plan" first issued in March 1996 and updated in June 1998, provides guidance and defines roles and responsibilities for addressing the Army Y2K problem. The plan supports the DoD Y2K Management Plan, which was first issued in April 1997 and updated in January 1999. Risk management is a process where the Component identifies and assesses the risk and plans for contingencies. As part of risk assessment, a Component must determine how a system may fail and how the failure will impact the system function or mission and affects on related interfacing systems Contingency plans are prepared based on risk assessments and identify detailed actions that will take place if a proposed Y2K correction fails or is not completed on time. There are two types of contingency plan: system and operational. System contingency plans were required by December 30, 1998, for all mission-critical systems undergoing renovation to become Y2K compliant. Components were also to prepare operational contingency plans for each core mission or function by March 31, 1999. Components must test both types of contingency plans by June 1999 to validate the information and procedures contained in the plan.

The DoD Y2K Management Plan includes questions that Components must answer to ensure that the plans they prepare are adequate. The questions address system description and mission, risks and impact of contingencies, resource requirements, degraded system functionality, impacts to hardware and software, and detailed solutions and workarounds.

System Contingency Plans

System contingency plans address processes and procedures to restore functionality to a system disrupted by the Y2K rollover, potential failure in systems believed to be Y2K compliant, interface failures, and failures in utilities and other systems necessary for operations, including workarounds to retain operations.

The ARNG prepared nine contingency plans from March 1998 through February 1999 for mission-critical systems that required modification to become Y2K compliant. The plans did not include sufficient system details, resource requirements such as training and funding, degraded system functionality, impacts to hardware and software, and detailed solutions and workarounds. In addition, the ARNG had not updated the plans to recognize changed requirements based on the changes in risk assessment and personnel.

While the ARNG made progress in preparing the plans, additional effort was needed. Unless the plans include all topics addressed in the DoD Y2K Management Plan, the continued operations of the system to accomplish its mission after the turn of the century is questionable.

Operational Contingency Plans

Operational contingency plans must address each Component's core missions or functions and identify alternative systems and procedures to complete the mission. The ARNG had prepared only the communications operational contingency plan, which is discussed in finding C. The ARNG planned to start a core functional analysis in January 1999 to determine critical functions, analyze processes, and prioritize missions. ARNG officials did not begin the analysis until May 1999, because of other Y2K priorities. The DoD Y2K Management Plan required the ARNG to complete the operational contingency plans by March 1999.

The ARNG must complete the analysis of mission-critical functions and complete the operational contingency plans to determine the number and types of operational contingency plans needed.

Testing

The DoD Y2K Management Plan requires a contingency plan to be tested before June 1999 to validate the information and procedures it contains. ARNG officials stated that they did not develop test plans or identify a testing schedule for system and operational contingency plans. The ARNG must schedule an exercise to test and prepare contingency test plans once the plans are updated and prepared. The contingency test results will provide confidence that the ARNG can meet its Federal and State obligations in the event of a Y2K disruption to the its systems.

Priorities

The Y2K problem was not assigned a level of awareness and a high enough priority that would have resulted in the preparation of complete and timely contingency plans. Project officials from the ARNG assigned to Y2K did not have direct authority over functional personnel involved in developing system and operational contingency plans and setting test schedules, making it difficult

to enforce DoD Y2K Management Plan requirements and deadlines. Not until October 1998 did the ARNG establish a task force to focus on Y2K issues. The task force focused on areas not addressed, such as the communications contingency plan, weapon systems, and installation mission support.

The ARNG should refocus its efforts and assign a high-ranking official at the ARNG to monitor the progress in establishing contingency plans and testing dates and to report monthly to the Director, ARNG.

Risk Management Plans

The ARNG did not prepare adequate risk management plans that would have allowed the ARNG to prepare adequate system contingency plans. All of the nine mission-critical systems that required a contingency plan had risk management plans. The plans, however, did not identify how a system or device could fail and how the failure would impact the system function or mission and, thus, the functions and missions of interfacing systems.

Because the risk assessments did not identify the impact of Y2K failures, including partial and full shutdown of the system, the contingency plan could not address all alternatives, resource requirements, degraded system functionality, and impacts to hardware and software. The ARNG must update the risk management plans to identify how a system or device may fail and how the failure could affect the system function or mission and the missions of interfacing systems.

Recommendations, Management Comments, and Audit Response

B. We recommend that the Director, Army National Guard:

1. Update the risk management plans to include how a system or device may fail and how the failure will affect the system function or mission and the functions and missions of interfacing systems.

2. Update the system contingency plans to include sufficient system details, resource requirements, degraded system functionality, impacts to hardware and software, and detailed solutions and workarounds.

3. Prepare a schedule to complete the analysis of mission-critical functions and complete the operational contingency plans.

4. Prepare test plans and schedule a test in a functional or operational exercise once the contingency plans are updated and prepared.

5. Assign a high-ranking official at the Army National Guard to monitor the progress in establishing contingency plans and testing dates and reports monthly to the Chief, National Guard Bureau.

Management Comments. The Director, ARNG, concurred with the finding and stated that each functional component has been tasked by the ARNG to upgrade the risk assessment and contingency plans and test the contingency plan by September 20, 1999. The Director also stated that, since the audit report was written the ARNG had begun to develop the headquarters operational contingency plan, which will include responsibilities and scenarios. The plan would be sent by the end of May 1999 to functional proponents to review their core business functions and provide detail annexes by September 1999. The Director also stated that the report attributed the delay in revising the plans to a lack of management priority, and that the report recommended a high ranking official monitor progress. He stated that the chief information officer, the Deputy Director, and he had monitored the Y2K program. He attributed the delay to the timing of other critical functions but agreed that it was time to refocus on the plans. The Assistant Secretary of Defense (Command, Control Communications and Intelligence) fully supported the finding and recommendations.

Audit Response. The comments of the Director, ARNG, were responsive to Recommendations B.1., B.2., B.3., and B.4. Regarding Recommendation B.5, the oversight described in the Director's response will meet the intent of the recommendation.

C. Operational Contingency Plan for Communication

The ARNG has made progress since the issuance of the draft audit report in ensuring its Communications Operational Contingency Plan could be implemented if communications failed because of Y2K disruptions. As a result, there is increased confidence that the ARNG communication ability will not be impaired.

Operational Contingency Plan Requirements

The "U.S. Army Y2K Action Plan" first issued in March 1996 and updated in June 1998, provides guidance for addressing the Army Y2K problem and supports the DoD Y2K Management Plan. The DoD Y2K Management Plan, first issued in April 1997 and updated in January 1999, states that Components must prepare operational contingency plans by March 31, 1999. Operational contingency plans address missions and identify alternative systems or procedures to use to complete the mission of a Component if the primary system fails because of Y2K disruptions. The DoD Y2K Management Plan provides a list of topics that each plan should embody, including vital functions, mission-critical systems that support the function, points of contact, procedures to detect corrupt data and report system faults, procedures to execute functions of the failed system, impact of the loss of the function, and links to other contingency plans.

Operational Contingency Plan for Communication

Communications is a vital mission of the ARNG because the Headquarters ARNG must be able to communicate with all 54 States and Territories to support Federal and State missions. The ARNG units now use mobile cellular telephones for communication. However, because of the potential for telephone system disruption in the year 2000, the ARNG prepared a draft communications operational contingency plan, November 1998. The contingency plan outlines a five-phase approach. During the first phase, completed in April 1999, the ARNG Headquarters, States and Territories, and their ARNG units completed a communication operations plan. This phase involved each unit planning for an exercise using high-frequency radio equipment to test connectivity between participants, setting up the equipment, and testing it to ensure proper operations. The second phase, completed in May 1999, tested the system to ensure total connectivity nationwide. The third phase, lasting until December 1999, will identify and solve system problems. Phase four will occur in December 1999 and involves 24-hour operation of the system on December 31, 1999, and maintenance until January 15, 2000, or until mission completion. Finally, phase five will involve a recovery and after-action review of the Y2K operation.

Funding and Testing for Communications Equipment

The recent test results of the Army in the May 1999 communications exercise demonstrated some success. The ARNG contacted 52 of the 54 States and Territories, had continuous voice communication with 22 of them, and had communication using automatic link establishment, both voice and data communications, with 23. The ARNG provided the other 32 States and Territories with $3.5 million to acquire the upgraded radios with automatic link establishments.

The success was without the originally planned $35 million in upgrades identified by the ARNG. Considering the test results for communications using equipment that the ARNG already owns and additional acquisitions, the ARNG has taken steps to ensure that its plan is achievable. ARNG officials stated that they have defined their communications requirements and will provide any additional funding requirements to the States and Territories as required.

Generators

All States do not have an adequate inventory of generators to provide power to National Guard armories if emergency housing or other emergency services are required. The locations of the shortages will not be identified and prioritized until August 1999. Each community and State must provide additional generators and resources if necessary. There were no excess generators in the Defense Reutilization Marketing Service Inventory as of February 17, 1999.

Conclusion

For a contingency plan to be effective, the solution must be implemented, funded, tested, and in place, when needed. Because the ARNG has made progress in implementing its plan, we are not making a recommendation.

Management Comments and Audit Response

Management Comments. The Director, ARNG, stated that the draft report incorrectly concluded that the Communications Operational Contingency Plan was at high risk of failure. The Director indicated that the May 1999 test results were positive. A high communication success rate existed without the benefits of additional funding for upgraded radios and antennas. As a result, the Director did not agree to a revised or rephased test plan, which the draft report recommended. The Assistant Secretary of Defense (Command, Control Communications and Intelligence) stated that he had contacted the ARNG and believes they are making progress in correcting many of the issues identified in the report. He also stated that the ARNG redirected funds to support its operational communication abilities.

Audit Response. The Communication Operational Contingency Plan provided to us during the audit had a high risk of failure due to the test schedule and the $35 million in funding needed to implement the plan. The May 1999 tests were positive and were without the benefit of upgrades the ARNG planned to acquire. As a result, we deleted the recommendations and revised the finding.

Appendix A. Audit Process

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 Y2K computing challenge. For a listing of audit projects addressing this issue, see the Y2K webpage on Ignet at http://www.ignet.gov.

Scope

Work Performed. We reviewed and evaluated the progress of the ARNG and the ARNG in resolving the Y2K computing issue. We evaluated their Y2K efforts compared with the DoD Y2K Management Plan; conducted discussions with technical, business, and contracting officials; and evaluated Y2K documentation where available.

DoD-Wide Corporate-Level Government Performance and Results Act Goals. In response to the Government Performance and Results Acts, the DoD has established 6 DoD-wide corporate level performance objectives and 14 goals for meeting those objectives. This report pertains to achievement of the following objective and goal.

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

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

Information Technology Management Functional Area.

- **Objective:** Provide services that satisfy customer information needs.
- **Goal:** Upgrade technology base. **(ITM-2-3)**

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

Methodology

Audit Type, Dates, and Standards. We performed this economy and efficiency 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 develop conclusions on this audit.

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

Management Control Program Review. 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

General Accounting Office and Inspector General, DoD. 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.

Army Audit Agency. The Army Audit Agency issued Report No. AA98-227, "Audit of Automated Information Systems Year 2000-U.S. ARNG," April 7, 1998. The report assessed the progress made in resolving Y2K problems especially addressing contingency planning and risks. The report identified that the ARNG did not prepare risk management or contingency plans for its mission-critical systems. Army officials agreed to prepare contingency plans based on risk assessments.

Appendix B. Description and Status of Mission-Critical Systems

Automated Fund Control Order System. The Automated Fund Control Order System is a finance system that publishes orders for ARNG personnel to perform active duty and travel. It provides complete financial management capabilities to program managers. The system was Y2K compliant as of December 31, 1998.

Aviation Logistic Readiness Model. The Aviation Logistic Readiness Model is a command and control system that encompasses the areas of aircraft maintenance, fiscal resource requirements, flying hour requirements, and execution data for ARNG aviators. The system was Y2K compliant as of December 31, 1998.

Joint Uniform Military Pay Service Standard Terminal Input System. The Joint Uniform Military Pay Service Standard Terminal Input System is a military pay system that interfaces with the Standard Installation and Division Personnel System processing personnel and pay transactions through the Defense Finance Accounting System. The system was Y2K compliant as of December 31, 1998.

Manpower Voucher System. The Manpower Voucher System provides manpower planning and programming in the National Guard. The system validates full-time employee requirements and produces staffing criteria. The system was Y2K compliant as of May 1999.

Reserve Component Management System-Guard. The Reserve Component Management System-Guard provides manpower, personnel, and resource management information to support decisionmaking for budget preparations and manpower projections and reports. The system was Y2K compliant as of May 1999.

Retirement Points Accounting Management System. The Retirement Points Accounting Management System provides retirement accounting, personnel management, and information retrieval. The system was in the implementation phase with an estimated Y2K implementation date of September 1999.

Standard Installation and Division Personnel System. The Standard Installation and Division Personnel System provides strength accounting, personnel management, information retrieval, and external interfaces at the unit operating level. The system was in the renovation phase with an estimated Y2K compliant as of May 1999.

State Accounting Budget Expenditure Reservation System. The State Accounting Budget Expenditure Reservation System accounts for funds received, obligated, and disbursed at the State level. The system was Y2K compliant as of February 5, 1999.

Total Army Personnel Database-ARNG. The Total Army Personnel Database-ARNG provides personnel data to support strength management for the ARNG Headquarters and detailed and summary level authorization and organization data. The system is part of the Total Army Personnel Functional Architecture to support and integrate personnel-related processes across the Army during peacetime, crisis contingency, and war. The system was Y2K compliant as of May 1999.

Training Readiness Operations Unit Planning Execution Resourcing System. The Training Readiness Operations Unit Planning Execution Resourcing System is a personnel readiness system that provides the States with a planning tool to manage annual training, schools, special training and inactive duty training. The system was Y2K compliant as of December 31, 1998.

User-Based ARNG System. The User-Based ARNG System is an environmental system that tracks hazardous material accumulations and provides reports to satisfy local and Environmental Protection Agency reporting requirements. The system was Y2K compliant as of December 31, 1998.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
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 Deputy - Y2K
Assistant Secretary of Defense (Reserve Affairs)
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Research, Development, and Acquisition)
Chief of Staff, Army
Chief, National Guard Bureau
  Director, Army National Guard
Chief Information Officer, Department of the Army
Inspector General, 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 Contract Audit Agency
Director, Defense Information Systems Agency
Inspector General, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Officer

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

Assistant Secretary of Defense (Command Control Communication and Intelligence) Comments

Final Report Reference

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

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

May 27, 1999

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT DIRECTORATE, INSPECTOR GENERAL DOD

SUBJECT: Comments on Audit Report on Y2K Conversion at the Army National Guard (Project No 9AB-0080)

I concur with your findings and recommendations to the Director, Army National Guard, as stated in the DRAFT report It is important for the Army National Guard to place the necessary emphasis on: system contingency plans and the necessary resources; mission-critical functions and operational contingency plans; test plans, tests and exercise schedules; appropriate officials to oversee, and report; update risk management plans; revise and re-phase communications contingency test plan; and provide sufficient resources to support contingency planning

Revised Page 10, 11

I would like to note your comments in Finding C - Operational Contingency Plan for Communications, "is at high risk of failure " Since your report, we have been in contact with the ANG and believe they are making good progress toward rectifying many of the issues you identified Their work to upgrade their high frequency equipment throughout the year, as well as the successes the ANG has experienced in recent exercises are good examples of the ANG's efforts We believe the ANG is taking the proper steps regarding its Communications Contingency Plan and is actively engaged A great deal of work remains and as your report indicates, funding is a critical issue for the ANG The ANG has been able to cope with this issue by redirecting operational funds to support its operational communications capabilities I believe the ANG has performed well in their aggressive awareness campaign, and in their work to ensure their extensive weapons inventory and Guard-unique systems are tested for Y2K compliance

I would like to again state my appreciation for your efforts and support in our informal partnership covering the Year 2000 computing problem My point of contact for any additional information in regarding the Army National Guard Audit Report is Mr Daniel Green at (703) 602-0991 ext 101, e-mail: Daniel Green@osd.pentagon.mil.

Marvin J Langston
Deputy Assistant Secretary of Defense
(Deputy CIO & Year 2000)

Army National Guard Comments

DEPARTMENTS OF THE ARMY AND THE AIR FORCE
NATIONAL GUARD BUREAU
1411 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22202 3231

NGB-IR (36-2c) 13 May 1999

MEMORANDUM THRU

U S Army Audit Agency, SAAG-PMO, ATTN Ms Sharon Trigueiro), 3101 Park Center Drive, Alexandria, VA 22302-1596

Director, Information Systems for Command, Control, Communications and Computers, ATTN SAIS-IM (COL John Thompson), 107 Army Pentagon, Washington, DC 20310-0107

FOR Inspector General, Department of Defense, 400 Army Navy Drive, Alexandria, VA 22202

SUBJECT Transmittal of Response for DODIG Audit Draft Report, Year 2000 Conversion Program at the Army National Guard (Project 9AB-0080)

1 The memorandum of response for SAB, dated 12 May 1999, is attached.

2. Any questions concerning this memorandum may be directed to Mrs Patricia A Gallop (703) 607-0180, e-mail gallopp@ngb ang.af mil, or Mr Lane G Haskew, (703) 607-0348, e-mail haskewl@ngb ang af mil

FOR THE CHIEF, NATIONAL GUARD BUREAU

Encl
as

for WALTER T. MORRISON
Director, Internal Review Directorate

DEPARTMENTS OF THE ARMY AND THE AIR FORCE
NATIONAL GUARD BUREAU
1411 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22202 3231

NGB-ARZ-DCI (25) 12 May 99

MEMORANDUM THRU

NATIONAL GUARD BUREAU CHIEF INFORMATION OFFICER, 1411 JEFFERSON DAVIS HIGHWAY, ARLINGTON, VA 22202-3231

CHIEF, NATIONAL GUARD BUREAU, 1411 JEFFERSON DAVIS HIGHWAY, ARLINGTON, VA 22202-3231

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

SUBJECT Audit report on Year 2000 Conversion Program at the Army National Guard (Project No 9AB-0080)

1. Reference memorandum, DoD IG, dated April 16, 1999, SAB.

2. Your office conducted a review of our Year 2000 (Y2K) and presented a final draft report on 16 Apr 99. The primary audit objective was to determine whether the Army National Guard was adequately preparing its information technology systems to resolve date-processing issues, and to focus on the administration of that portion of our program We concur with your findings on our Contingency Plans, and have introduced changes to our program to fix these deficiencies. We do not concur, however, with your findings regarding the communications exercise (COMEX) We also believe that the scope of the audit excluded many successful initiatives that have been vital in preparation for any potential Y2K disruptions.

3 Let me start by addressing the areas that the audit did not cover. We have had an aggressive awareness campaign, coordinated with the National Guard Bureau Public Affairs Office, that included presentations at the Senior Leadership Conference, Director of Information Management Conference, United States Property & Fiscal Office Conference, and newspaper advertisements We have taken time to check our weapons inventories for Guard-unique systems to ensure that they are tested for Y2K compliance I have personally contacted the State Adjutants General to solicit their support in working installation support issues including fire, safety, and responses to local utility failures We have also been actively involved in canvassing the 54 States,

Territories, and the District of Columbia to ensure that their presumptions on how to use their forces in support of Y2K do not conflict with Federal requirements. Each of these programmatic areas is critical to the success of Y2K as a whole, yet none were included in the scope to this audit.

4. We concur with Finding A regarding compliance of mission -critical systems. Five of our systems did not meet the Office of Management and Budget's 31 Mar 99 deadline for certification. Since the report was written, three of those systems have been certified (MANPOWER-VOUCHER Redesign, RCMS-GUARD, and TAPDB-ARNG). We expect SIDPERS-ARNG to be certified by 30 May 99. The certification date for RPAM has changed to 1 Sep 99, and work on that system continues under the direction of the National Guard Bureau Program Executive Officer for Information Systems. It receives the highest levels of attention daily.

5 We concur with most of Finding B regarding System Contingency Plans and our headquarters Operational Contingency Plan. It is important to review and upgrade Risk Assessment Plans and System Contingency Plans for our critical systems. Each functional proponent has been tasked to upgrade these plans and conduct a test of their System Contingency Plan by 30 Sep 99. Since the draft report was written, we have started the development of the headquarters Operational Contingency Plan. The base plan, with responsibilities and potential Y2K scenarios, will be sent to functional proponents for their action by 21 May 99. Functional proponents will review their core business functions and provide their detailed annexes to my Deputy Director by 1 Sep 99.

6. Finding B attributed much of the delay in revising these plans to a lack of management priority. It further recommends that the Army National Guard assign a high-ranking official to monitor progress. The Army National Guard Chief Information Officer has continually kept a pulse on the program, my Deputy Director has verified all Certification packets for critical systems, and I have been personally involved as needed. We have had a delay in upgrading Contingency Plans because the timing of other critical functions, outlined earlier in the letter, took priority. We agree with the report when it states that it is time to refocus on these plans. That was always our intention, and we believe we now have enough other portions of the program in place to concentrate on ensuring our Contingency Plans are truly accurate and meaningful.

Final Report Reference

NGB-ARZ-DCI
SUBJECT: Audit report on Year 2000 Conversion Program at the Army National Guard (Project No. 9AB-0080)

Revised 10, 11

7 In the last finding (Finding C), the report contends that the Communications Operational Contingency Plan is at high risk of failure. We have just concluded the initial COMEX and demonstrated a great degree of success. We contacted 52 of 54 States (96%); had continuous voice with 22 of 54 States (40%), and had continuous voice communications using Automatic Link Establishment (ALE) with 23 of 54 States (42%). At least once during the May 99 COMEX, we had 91% of the stations in the network up and running. These results were achieved without the favorable impact of funds distributed to each State/Territory for upgrade of radios and antennas that will support this net. We will continue to upgrade our high frequency equipment throughout the year. For this reason, I do not believe that we need to revise or rephase the test plan.

8. We share your concerns with funding for our COMEX and for our entire Y2K program. Even with the Congressional Supplement of $3.5 million, we have had to redirect operational funds to support the COMEX. We continue to redirect maintenance funds to complete software, perform hardware upgrades, and complete required testing.

9. We will continue to press on with our Y2K program and ensure that we are ready to meet the challenges of the new year.

10. The point of contact for this action is LTC Kirk Krist, (703)607-0163.

FOR THE CHIEF, NATIONAL GUARD BUREAU:

ROGER C. SCHULTZ
Major General, GS
Director, Army National Guard

3

Audit Team Members

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

Thomas F. Gimble
Patricia A. Brannin
Raymond A. Spencer
Michael E. Simpson
Lisa E. Novis
Ronald L. Nickens
Barbara A. Moody
Krista S. Gordon
Bernice M. Lewis