Audit Report

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

YEAR 2000 CONTINGENCY PLANNING AND OPERATIONAL EVALUATION REPORTING BY U.S. FORCES KOREA

Report No. D-2000-029 November 1, 1999

Office of the Inspector General
Department of Defense

DTIC QUALITY INSPECTED 1

20000209 107

AQI00-05-1190

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Year 2000 Contingency Planning and Operational Evaluation Reporting by U.S. Forces Korea

B. DATE Report Downloaded From the Internet: 02/08/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 02/08/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

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, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

OPEVAL	Operational Evaluation
ROK	Republic of Korea
USFK	U.S. Forces Korea
Y2K	Year 2000

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

November 1, 1999

MEMORANDUM FOR COMMANDER IN CHIEF, U.S. FORCES KOREA

SUBJECT: Audit Report on Year 2000 Contingency Planning and Operational Evaluation Reporting by U.S. Forces Korea (Report No. D-2000-029)

We are providing this report for information and use. This report is one of a series resulting from our audit of "Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility." Under current plans, it is the last report of the series. This report discusses year 2000 contingency planning efforts and operational evaluation reporting by U.S. Forces Korea. We considered management comments on a draft of this report in preparing the final report.

Management comments on the draft report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Robert M. Murrell at (703) 604-9210 (DSN 664-9210) (rmurrell@dodig.osd.mil) or Mr. Patrick J. Nix at (703) 604-9290 (DSN 664-9290) (pnix@dodig.osd.mil). See Appendix D 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-2000-029 **November 1, 1999**
(Project No. 8CC-0049.09)

Year 2000 Contingency Planning and Operational Evaluation Reporting by U.S. Forces Korea

Executive Summary

Introduction. This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge. For a list of audit projects addressing the issue, see the year 2000 web pages on the IGnet at http://www.ignet.gov.

Objectives. The overall audit objective was to evaluate whether the U.S. Pacific Command adequately planned for and managed year 2000 risks to avoid disruptions to its mission. Specifically, we evaluated U.S. Forces Korea's contingency planning and operational evaluation reporting efforts.

Results. U.S. Forces Korea and its subordinate organizations made significant progress toward ensuring mission capability through the year 2000 transition period. Like other DoD Components, U.S. Forces Korea and its subordinate organizations needed to keep working through the time period remaining before January 2000 to maximize confidence in continued high readiness. Specifically, U.S. Forces Korea and its subordinate organizations had not yet finalized and exercised all the year 2000 contingency plans supporting critical missions to ensure that viable plans and sufficient resources were in place. In addition, workarounds for year 2000 contingency plans had not yet been prioritized to ensure critical mission accomplishment if resources prove inadequate or fully coordinated to ensure sufficient resources were in place to accomplish the most critical missions, if workarounds are implemented simultaneously. U.S. Forces Korea subsequently took actions to address those concerns. For details of the audit results, see finding A.

U.S. Forces Korea correctly reported to the Joint Staff known failures and anomalies identified by its first operational evaluation. However, operators did not record events as the events occurred, data collectors did not adequately document data collected or perform thorough quality assurance reviews, and operational evaluation personnel did not perform sufficient analysis of the data captured. Although U.S. Forces Korea identified those as lessons learned and planned to improve its training and data analysis procedures for its second operational evaluation, year 2000-related failures and anomalies that occurred during U.S. Forces Korea's first operational evaluation may not have been identified. U.S. Forces Korea subsequently took actions to address those concerns. For details of the audit results, see finding B.

Summary of Recommendations. We recommend that the Commander in Chief, U.S. Forces Korea, finalize, review, and exercise year 2000 contingency plans, and prioritize and coordinate the workarounds outlined in those plans, to ensure viable

plans and sufficient resources are in place to enable the successful accomplishment of U.S. Forces Korea's most critical missions should the workarounds be employed simultaneously.

We also recommend that the Commander in Chief, U.S. Forces Korea, ensure operators and data collectors are trained on data collection procedures and develop more specific procedures for recording events, conducting analysis, and performing quality assurance reviews of data collections for the second operational evaluation.

Management Comments. U.S. Forces Korea concurred with the finding and recommendations addressing U.S. Forces Korea's contingency planning efforts. U.S. Forces Korea stated corrective actions were ongoing to finalize and exercise all year 2000 contingency plans supporting U.S. Forces Korea critical missions and systems. U.S. Forces Korea also stated the contingency plans were being reviewed to ensure their adequacy, that the plans were supported by viable and sufficient resources, and that a plan was in place to prioritize and coordinate resource requirements to enable the simultaneous accomplishment of critical missions.

U.S. Forces Korea partially concurred with the finding and recommendations addressing its operational evaluation reporting, stating corrective actions were taken to improve its training and procedures. U.S. Forces Korea stated it had made major adjustments in the preparation of its second operational evaluation. Specifically, data collectors and operators received detailed training on their roles and the tasks to be performed. Further, the data collectors at each site and personnel at an analysis cell conducted real-time analysis of the data collected. In addition, a baseline comparison was made to validate that the procedures used by the data collectors were effective and a comparison of sent and received products was made to analyze the timeliness, completeness, and accuracy of the data collected. A discussion of management comments is in the Findings section of the report and the complete text is in the Management Comments section.

Audit Response. Comments from U.S. Forces Korea are responsive; therefore, no additional comments are required.

Table of Contents

Executive Summary i

Introduction

Background 1
Objectives 2

Findings

A. U.S. Forces Korea's Year 2000 Contingency Planning Efforts 3
B. U.S. Forces Korea's Year 2000 Operational Evaluation Reporting Efforts 9

Appendixes

A. Audit Process Scope and Methodology 15
B. Summary of Prior Coverage 17
C. Host Nation Support 18
D. Report Distribution 19

Management Comments

U.S. Forces Korea 23

Background

This report is the 10th in a series resulting from our audit of "Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility." This report discusses year 2000 (Y2K) contingency planning and operational evaluation reporting efforts by U.S. Forces Korea (USFK). Under current plans, this is the last report of the series. Other reports in the series that have been issued as final reports are identified in Appendix B.

DoD Y2K Management Strategy. In his role as the DoD Chief Information Officer, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) is coordinating the overall DoD Y2K conversion effort. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued various iterations of a Y2K management plan to provide direction and make the DoD Components responsible for implementing the five-phase Y2K management process. The "DoD Year 2000 Management Plan, Version 2.0," December 1998, is the most current iteration.

The Joint Chiefs of Staff. The Chairman of the Joint Chiefs of Staff is the principal military adviser to the President, the Secretary of Defense, and the National Security Council. The Secretaries of the Military Departments assign all forces under their jurisdiction to the unified commands to perform missions assigned to those commands. The Joint Staff assists the Chairman of the Joint Chiefs of Staff with unified strategic direction of the combatant forces; unified operation of the combatant commands; and integration into an efficient team of air, land, and sea forces.

U.S. Pacific Command. The U.S. Pacific Command is the largest of the nine unified commands of the Department of Defense. It was established as a unified command on January 1, 1947, as an outgrowth of the command structure used during World War II. The U.S. Pacific Command area of responsibility includes 50 percent of the earth's surface and two-thirds of the world's population. It encompasses more than 100 million square miles, stretching from the west coast of North and South America to the east coast of Africa and from the Arctic in the north to the Antarctic in the south. It also includes Alaska, Hawaii, and eight U.S. territories. The overall mission of the U.S. Pacific Command is to promote peace, deter aggression, respond to crises, and, if necessary, fight and win to advance security and stability throughout the Asian-Pacific region.

The U.S. Pacific Command, located at Camp H.M. Smith, Hawaii, is supported by Component commands from each Service: U.S. Army Pacific, U.S. Pacific Fleet, U.S. Pacific Air Forces, and U.S. Marine Forces Pacific. In addition, the U.S. Pacific Command exercises combatant command over four sub-unified commands within the region. The sub-unified commands are U.S. Forces Japan, USFK, Alaskan Command, and Special Operations Command Pacific.

U.S. Forces Korea. USFK was established in July 1957 as an outgrowth of the longtime U.S. security commitment to the Republic of Korea (ROK). The commitment began at the end of World War II when U.S. troops entered Korea to accept the surrender of Japanese forces in the zone south of the 38th parallel.

The U.S. security commitment has legal obligations based on the United Nations Security Council Resolution of 1950, which tasked the United States to provide the commander of the United Nations Command, and the ROK/U.S. Mutual Security Agreement of 1954, which commits both countries to assist each other in the event of outside attack. The USFK was established as the planning headquarters to coordinate joint service activities of U.S. forces in the ROK. The United States is also a partner in the operations of the ROK/U.S. Combined Forces Command, which was activated by the two governments in November 1978.

The Combined Forces Command is a totally integrated headquarters responsible for planning the defense of the ROK and, in case of hostilities, directing the ROK/U.S. combat forces (about 650,000 ROK Armed Forces and 37,000 U.S. Service personnel) to defeat enemy aggression. With the activation of Combined Forces Command, USFK became the headquarters through which U.S. combat forces would be mobilized to augment the Combined Forces Command fighting components. USFK includes all U.S. Army, Navy, Air Force, and Marine elements stationed in Korea. The Commander in Chief, USFK, also serves as commander of the United Nations Command and the Combined Forces Command.

Objectives

The overall audit objective was to evaluate whether the U.S. Pacific Command adequately planned for and managed Y2K risks to avoid disruptions to its mission. Specifically, in this phase of the audit, we evaluated the contingency planning and operational evaluation (OPEVAL) reporting efforts by USFK. See Appendix A for a discussion of the audit scope and methodology, Appendix B for a summary of prior coverage, and Appendix C for a discussion on the USFK host nation support efforts.

A. U.S. Forces Korea's Year 2000 Contingency Planning Efforts

USFK and its subordinate organizations made significant progress toward ensuring mission capability through the Y2K transition period. Additional efforts, including a planned second OPEVAL, were needed to maximize confidence in continued high readiness. Specifically, USFK and its subordinate organizations had not yet finalized and exercised all Y2K contingency plans supporting USFK critical missions to ensure viable plans and sufficient resources were in place to enable the successful accomplishment of critical missions. Further, workarounds for Y2K contingency plans had not yet been prioritized to ensure critical mission accomplishment if resources prove inadequate or fully coordinated to ensure sufficient resources were in place, if workarounds are implemented simultaneously. Contingency plans were not always developed and exercised, and workarounds were not prioritized because not all DoD organizations within Korea adhered to pertinent guidance, and USFK had not developed plans to identify the resources required by the simultaneous execution of more than one workaround. As a result, continued command emphasis is needed.

Y2K Contingency Plans

DoD is making extraordinary efforts to meet the technical challenges associated with Y2K compliance. However, despite those efforts, there is no guarantee that all DoD systems will be fully compliant and free of risk by January 1, 2000. Systems that have been renovated could fail, and the failure of one system could disrupt many others. In addition, infrastructure disruptions could prevent a system from performing, even if the system itself is capable of correctly processing all data. Contingency plans address many of the possible types of Y2K-related disruptions, ensuring that procedures are in place to expedite the restoration of the system and to continue the mission or function if system support is not available, regardless of the reason of the disruption.

The purpose of a contingency plan is to provide a road map of predetermined actions that will streamline decisionmaking during the contingency to enable resumption of mission operations at the earliest possible time. Good planning will reduce the number and magnitude of decisions that must be made during the period immediately following a disruption, when exposure to error is at its peak. Contingency plans establish, organize, and document risk assessments, responsibilities, policies, and procedures, as well as agreements and understandings for all internal and external entities. Personnel should be trained in the execution of contingency plans, and the plans should be tested and updated periodically to ensure that plans remain current and valid. There are two types of Y2K contingency plans: system contingency plans and operational contingency plans.

System Y2K Contingency Plans. System Y2K contingency plans address the technical aspects of potential disruptions in systems believed to be Y2K compliant. The sources of such disruptions may include interface failures, transmission or receipt of corrupt data, or problems with utilities or other infrastructure support necessary for operation. System Y2K contingency plans should include technical workarounds necessary to recover the system or to use other system capabilities to meet customers' requirements to sustain missions. System Y2K contingency plans are required for all mission-critical systems.

Operational Y2K Contingency Plans. Operational Y2K contingency plans (also known as continuity of operations plans) address continuing and completing missions or functions when any of the supporting mission systems are disrupted. The plans are developed to enable the continuation and completion of missions and functions under "worst case" circumstances. Each core mission or function or critical process should have an operational Y2K contingency plan. Operational Y2K contingency plans are developed and executed by the group responsible for executing the core mission process. The plans should include alternative procedures and workarounds necessary to execute the mission or function at or above minimum acceptable levels of functionality.

Mission-critical system contingency plans and operational contingency plans were to be completed by December 30, 1998, and March 31, 1999, respectively, and all plans should have been tested to ensure their viability before June 30, 1999. Few DoD Components were able to achieve those goals.

Developing and Exercising Y2K Contingency Plans

USFK and its subordinate organizations made significant progress in their contingency planning efforts. However, USFK and its subordinate organizations had not yet finalized and exercised all Y2K contingency plans supporting USFK critical missions to ensure viable plans and sufficient resources were in place to enable the successful accomplishment of USFK critical missions.

Developing Y2K Contingency Plans. The Technical Management Branch within the USFK Y2K task force was responsible for monitoring the progress of Y2K contingency planning efforts. It issued supplemental guidance and provided training to the USFK functional staff and subordinate organizations on developing and testing Y2K contingency plans. Further, it tasked the USFK functional staff and subordinate organizations to submit their Y2K contingency plans for review by the USFK Y2K task force by April 1, 1999. As of July 1999, the Technical Management Branch had received 123 of the 145 Y2K contingency plans that were to be developed for expediting the restoration of critical system support interrupted as a result of Y2K problems and for ensuring the continuity of USFK critical missions while system support is unavailable. The Technical Management Branch was in the process of evaluating the viability of the 123 Y2K contingency plans it had received.

USFK and its subordinate organizations were still finalizing the remaining 22 Y2K contingency plans. For example, the Y2K focal points for the USFK logistics and intelligence directorates, the 19th Theater Area Army Command, and the Defense Information Systems Agency, Korea, stated they either had not prepared the Y2K contingency plans yet, did not have the plans for use in theater, or were still finalizing the workarounds contained in the plans for systems or processes that were critical to USFK. The USFK Y2K task force needs to task the USFK functional elements and subordinate organizations to finalize their contingency plans and complete its review of the adequacy of the plans.

Exercising Y2K Contingency Plans. The Eighth U.S. Army and the 19th Theater Area Army Command had not exercised the Y2K contingency plans that had been developed to ensure continuity of the critical tasks associated with the logistics function. The contingency plan workarounds require users to revert to manual procedures to overcome system disruptions. The Eighth U.S. Army and the 19th Theater Area Army Command should exercise the plans to ensure sufficient resources are on hand to successfully accomplish critical logistics tasks. In another example, the Y2K focal points for USFK and Eighth U.S. Army operations directorates stated they were going to use the USFK OPEVALs to test their Y2K contingency plans. However, those Y2K contingency plans would be exercised during those OPEVALs only if critical system support is lost as a result of Y2K problems. Therefore, if system support is not lost during the USFK OPEVALs and those plans do not get exercised, then other methods should be used to evaluate the viability of the workarounds. The USFK Y2K task force needs to task the USFK functional elements and subordinate organizations to exercise all Y2K contingency plans for critical missions and systems to ensure viable plans and sufficient resources are in place to enable the successful accomplishment of USFK critical missions.

Prioritization and Coordination of Y2K Contingency Plans

Y2K contingency plan workarounds for ensuring mission continuity had been neither prioritized to ensure the successful accomplishment of critical USFK missions if resources prove inadequate, nor fully coordinated to ensure sufficient resources were in place to accomplish the most critical missions if workaround measures are implemented simultaneously.

Prioritization of Contingency Plans. USFK had not fully identified and assessed the resources required to implement workarounds for the Y2K contingency plans of all USFK functional elements or subordinate organizations and, as a result, had not initiated plans to prioritize those resource requirements should resources prove inadequate.

We reviewed the workarounds identified in 56 of the 123 Y2K contingency plans developed to restore critical USFK system support and to continue USFK critical missions in the event of a system failure. We identified a number of DoD organizations in Korea that plan to employ the same resources to continue their missions if system support is not available as a result of Y2K-related

failures. Of the 56 contingency plans we reviewed, 20 plans were system Y2K contingency plans and, thus, did not require operational workarounds. Workarounds in the remaining 36 plans identified 7 communications and information exchange systems and other assets for use in the event of system failures as a result of Y2K problems. The following table shows the 7 communications and information exchange systems and other assets designated for either primary or secondary use in workarounds by the 36 Y2K contingency plans.

Communications Systems and Other Assets Designated as Workarounds in Y2K Contingency Plans of USFK and Its Subordinate Organizations

System or Other Asset	Primary Workaround*	Secondary Workaround*
Automatic Digital Network	0	1
Courier	0	5
Defense Switched Network with Secure Telephone Unit and fax	5	18
High Frequency Radio Communications	0	5
Personal Computer	13	3
Secret Internet Protocol Router Network/ Unclassified but Sensitive Internet Protocol Router Network	23	4
Typewriter	0	12

*Some Y2K contingency plans required multiple communications systems and other assets to accomplish critical tasks using workarounds.

Communications systems, within not only Korea but throughout DoD, may experience widespread infrastructure problems as a result of Y2K problems and may cause many commands to simultaneously implement workaround measures using the same systems and assets. Therefore, USFK should not presume that all seven communications systems and other assets would be available for use as workarounds for the period immediately following January 1, 2000. USFK should prioritize workaround requirements identified in Y2K contingency plans to ensure limited resources are allocated to its most critical missions, functions, and processes. Once prioritization of workaround requirements has been accomplished, coordination must be performed to reallocate available resources.

Coordination of Contingency Plans. As of July 1999, the USFK Y2K task force and USFK subordinate organizations had not initiated plans to coordinate resource requirements identified in Y2K contingency plans for all USFK functional elements or subordinate organizations. There is no guarantee that all systems within USFK will be fully compliant and free of risk by January 1, 2000, and the potential for multiple failures of systems required for critical missions, functions, and processes needs to be considered in USFK contingency planning. Coordinated planning would allow workarounds to be accomplished

simultaneously, should circumstances involving multiple system failures dictate that be needed. USFK, in conjunction with its subordinate organizations, needed to fully coordinate Y2K contingency plans to ensure that resources required by more than one workaround were identified and resources were allocated to ensure the accomplishment of the most critical USFK missions should workarounds be implemented simultaneously.

Conclusion

USFK, and its subordinate organizations, made significant progress toward ensuring mission capability through the Y2K transition period. However, as is the case with most other DoD Components, additional efforts were required or advisable to ensure critical mission continuity. USFK needed to finalize and exercise all of the Y2K contingency plans supporting USFK critical missions to ensure viable plans and sufficient resources are in place to enable the successful accomplishment of those missions. In addition, USFK needed to prioritize and coordinate Y2K contingency plan workarounds to ensure sufficient resources are in place for the accomplishment of critical missions should workarounds be implemented simultaneously.

Recommendations, Management Comments, and Audit Response

A. We recommend that the Commander in Chief, U.S. Forces Korea:

1. Finalize year 2000 contingency plans that have not yet been completed for critical missions and systems.

2. Complete the review of the adequacy of year 2000 contingency plans for critical missions and systems.

3. Complete the exercising of all year 2000 contingency plans for critical missions and systems to ensure viable plans and sufficient resources are in place to enable the successful accomplishment of U.S. Forces Korea's critical missions.

4. Prioritize and coordinate the workarounds outlined in year 2000 contingency plans to ensure sufficient resources are in place to enable successful execution of critical missions, functions, and processes should the workarounds be employed simultaneously.

Management Comments. USFK concurred with the finding and recommendations, stating corrective actions were ongoing to finalize and exercise all the Y2K contingency plans supporting USFK critical missions and systems. Those efforts are scheduled to be completed in November 1999. USFK also stated the contingency plans were being reviewed to ensure their

adequacy, that the plans were supported by viable and sufficient resources, and that a plan was in place to prioritize and coordinate resource requirements to enable the simultaneous accomplishment of critical missions.

B. U.S. Forces Korea's Year 2000 Operational Evaluation Reporting

USFK correctly reported to the Joint Staff known Y2K-related failures and anomalies identified by its first OPEVAL. However, operators did not record events as the events occurred, data collectors did not adequately document data collected or perform thorough quality assurance reviews, and OPEVAL personnel did not perform sufficient analysis of the data captured. Events were not recorded as the events occurred, data were inadequately documented, and thorough quality assurance checks were not performed because USFK OPEVAL team training was ineffective. Further, OPEVAL personnel did not perform sufficient analysis because data analysis procedures were faulty. As a result, there was no assurance that all Y2K-related failures and anomalies that occurred during the first OPEVAL were identified. USFK recognized those deficiencies as lessons learned from the first OPEVAL.

Y2K Operational Evaluation

Public Law 105-261, "Strom Thurmond National Defense Authorization Act for Fiscal Year 1999," October 17, 1998, directed the Secretary of Defense to ensure that at least 25 military exercises, to be conducted in the first 9 months of 1999, include a simulated Y2K phase; at least 2 of the 25 exercises be conducted by the commander of each unified or specified combatant command; and all mission-critical systems expected to be used if the Armed Forces were involved in a major theater war be tested in at least 2 exercises. The objective of those requirements was to operationally evaluate the extent to which information technology and national security systems will successfully operate during the year 2000. The public law allows information technology or national security systems to be excluded from the Y2K simulation phase of exercises if the systems are incapable of performing reliably in a Y2K environment. However, in those cases, the excluded systems must be replaced in accordance with the measures outlined in the systems' Y2K contingency plans.

The Joint Staff developed a multifaceted assessment program that combines testing conducted at Office of the Secretary of Defense, Joint Staff, unified command, Service, and agency levels to implement the requirements of Public Law 105-261. The Joint Staff program assigns the unified commands the responsibility for conducting Y2K mission-centric evaluations of the various "thin-lines of systems" critical to the performance of operational missions. To comply with Public Law 105-261 and the Joint Staff's guidance, USFK planned to conduct two OPEVALs to verify that it can successfully execute the missions, functions, and tasks critical to major theater war operations in a Y2K environment. The first of the USFK OPEVALs occurred in April 1999 and the second one in September 1999.

USFK evaluated 6 of its 15 thin-lines critical to major theater war operations in its first OPEVAL. The evaluation was accomplished through execution of a Master Scenario Event List. The Master Scenario Event List integrated all six thin-lines into a single test string, allowing for near simultaneous testing representative of real world operational conditions. The Master Scenario Event List was executed 24 times during the OPEVAL, once during every data collection period.

Operational Evaluation Reporting

USFK correctly reported known Y2K-related failures and anomalies identified by its OPEVAL to the Joint Staff. USFK evaluation of the data collection products uncovered two Y2K-related anomalies that occurred in the first OPEVAL. USFK correctly informed the Joint Staff of those anomalies in its final report on the OPEVAL.

USFK used event list logs, computer screen captures, and task observation and system evaluation templates to document the results of the OPEVAL. Event list logs were used to identify the organizations transmitting and receiving data products, the alternative actions taken to accomplish the data transfer if anomalies occurred that prevented transmission or receipt of data using the primary communications medium, the scenario times, and the local times. Computer screen captures were taken to obtain hard-copy evidence of the data transmitted and received, in addition to the time of occurrence according to the system's clock display. Task observation templates were used to identify the thin-line and task being evaluated, the data capture location, the run sequence, and whether or not there were any problems or failures observed during the OPEVAL execution. System evaluation templates were used to identify the systems being evaluated, the data capture location, and whether or not any failures or anomalies occurred during the various OPEVAL runs.

Operational Evaluation Team Training

Operators did not record events on the event list logs as they occurred and data collectors did not adequately document the resolution of deviations on task observation and system evaluation templates or perform thorough quality assurance reviews. Events were not recorded as the events occurred, data were inadequately documented, and thorough quality assurance checks were not performed because USFK OPEVAL team training was ineffective. USFK OPEVAL team training was ineffective because it did not adequately acquaint operators with the procedures for recording the times that data transmissions and receipts occurred, did not adequately acquaint data collectors with their data documentation and quality assurance duties, and did not adequately acquaint ROK participants with the data collection requirements.

Operator Training. Operators were responsible for writing down anything that deviated from the normal day-to-day functions of their workstations. If problems arose, the operators were to notify the data collectors and log anything that could have been or was a degradation of information on the task observation template. The operators were also to fill out the event list as they completed tasks and obtained computer screen captures. Screen captures were particularly significant because the captures provided the most relevant and reliable data collected for analysis of transmission time. The instructions on how the task observation templates and event list logs were to be filled out were contained within those documents.

Documentation Procedures. Operators were unfamiliar with the documentation procedures for capturing data transmission times. Operators did not consistently capture accurate times when data were transmitted and received. Variations existed in transmission and receipt times recorded by screen captures and in the event list logs. For example, our review of the data for one thin-line revealed seven instances where the event list logs and computer screen captures showed receipt times that preceded their corresponding transmission times. Further, analysis of two thin-lines revealed that the amount of time taken for destination locations to receive data transmissions differed greatly for each of the 24 executions of the Master Scenario Event List. For example, the elapsed times of transmitted messages for the Master Scenario Event List executions for one event within a thin-line ranged from negative 0.5 minutes to 54.6 minutes, with the elapsed transmission time for only one execution falling within the baseline established by USFK. According to USFK OPEVAL team officials, those differences were because operators did not record data transmissions and receipts when they actually occurred.

Time Comparison. The procedural deviations in documenting times resulted in the loss of time comparison as an analysis tool. The USFK OPEVAL team could not effectively compare the times taken to receive data with the baselines in order to isolate transmission time lags that may have resulted from Y2K-related anomalies. USFK correctly identified those deviations as lessons learned. USFK plans to stress the importance of time as an analysis tool for detecting Y2K-related anomalies and emphasize the need of operators to accurately record transmission and receipt times as a part of its OPEVAL team training for its second OPEVAL.

Data Collector Training. Data collectors were responsible for the monitoring and gathering of the specific data collection products. If any systems experienced a problem, the data collector was to notify the appropriate technicians, inform the Combined Exercise Control Staff, and adequately document the problem on the appropriate system evaluation template. The data collectors were then to record the fact if the technicians diagnosed the problem as mechanical. Further, if the technicians were able to resolve the problem, the data collectors were to so note on the system evaluation template. The data collectors were to also perform quality assurance checks of all data collection products to ensure that the products were complete. Procedures were in place to capture and document event data for future analysis and for use by the data collectors to ensure the proper processing of data collection forms.

Resolution of Problems. Data collectors did not document the resolution of problems that occurred during the OPEVAL. Problems were annotated in the margins of the event list logs; however, explanations of how the problems were resolved and the conditions under which the problems occurred were missing. Further, the annotations did not include the impact of the problems on system services and capabilities, or mention any subsequent workarounds attempted. Data collectors' annotations included:

- connectivity problems,
- invalid year warnings,
- power outages,
- physical memory dump anomaly,
- no computer screen capture, and
- wrong integrated tasking order captured.

Quality Assurance Reviews. The execution of quality assurance reviews should have discovered those annotation deficiencies. However, the data collectors did not conduct thorough quality assurance reviews. USFK correctly identified the shortcomings of the data collectors' grasp of documentation requirements and their quality assurance duties as lessons learned. USFK expected to improve those areas of training for data collectors for its second OPEVAL.

ROK Participant Training. The operator at one of the two ROK organizations participating in the first USFK OPEVAL was not fully apprised of all the data collection procedures for operators. As a result, the operator did not complete event list logs for his data collection location. USFK OPEVAL officials believe the ROK confusion over the data collection procedures was a direct result of the shortcomings in the USFK OPEVAL team training. USFK provided its OPEVAL team training in English; it did not provide a translator for the ROK participants. USFK expected to provide bilingual training to the representatives from the ROK organizations participating in its second OPEVAL.

Data Analysis Procedures and Methodology

OPEVAL personnel did not perform sufficient analysis of the data captured because data analysis procedures were faulty. USFK analysis procedures did not include comparison of the data collected with baselines, and the methodology used for identifying soft failures contained in OPEVAL messages was not effective.

Baseline Comparison. USFK did not compare OPEVAL data collected with established baselines to identify potential soft failures resulting from Y2K-corrupted data that may have been contained in the databases from which

the OPEVAL messages were created. For example, USFK OPEVAL personnel did not detect an anomaly contained in one of the messages transmitted to test one of the thin-lines. Although a system operator manually changing flight altitudes contained in the standard baseline message caused the anomaly, it could have just as easily been caused by Y2K-corrupted data contained in the database used to store the standard message. OPEVAL officials stated that the anomaly should have been reported as a deviation and investigated. A comparison of the messages received at the destination locations with established baselines would have provided USFK the means to detect that anomaly and others like it. USFK needs to incorporate into its data analysis procedures a comparison of the OPEVAL messages transmitted with established baselines.

Methodology. The methodology used by USFK for identifying soft failures contained in OPEVAL messages was not effective. USFK relied on visual comparison of messages transmitted with messages received to identify soft failures contained in OPEVAL message traffic. The lack of an automated comparison tool created an environment in which soft failures could easily remain undetected. For example, the messages transmitted to accomplish a critical task supported by one thin-line consisted of lengthy numeric and alphanumeric character strings and detailed mission numbers. The visual caparison methodology used by USFK for detecting soft failures could have easily failed to detect soft failures contained in those messages. USFK OPEVAL personnel expressed a desire to automate the analysis of OPEVAL messages, which would greatly increase the assurance that potential irregularities contained in highly detailed messages could be promptly detected.

Conclusion

USFK correctly reported known Y2K-related failures and anomalies identified by its first OPEVAL to the Joint Staff. However, improved training and data analysis procedures were required to ensure all Y2K-related failures and anomalies occurring in the second USFK OPEVAL are identified. USFK needed to increase OPEVAL system operators' awareness of the importance of accurate time documentation and computer screen captures, improve data collectors' training of data documentation and quality assurance requirements, and expand data analysis procedures to include a baseline comparison and automated review of OPEVAL data.

Recommendations, Management Comments, and Audit Response

B. We recommend that the Commander in Chief, U.S. Forces Korea:

1. Ensure that operators and data collectors are properly trained on the implementation of data collection procedures in preparation for the second operational evaluation.

Management Comments. USFK concurred, stating corrective actions were taken to improve its training and procedures. USFK stated data collectors and operators received detailed training on their roles and the tasks to be performed and were provided printed guidance for use in the second OPEVAL. USFK stated those actions and a practical exercise and rehearsal conducted helped correct problems identified during the first OPEVAL.

2. Develop more specific data analysis procedures for conducting the second operational evaluation, to include the automated comparison of operational evaluation results with established baselines.

Management Comments. USFK partially concurred, stating that the analysis procedures used in the second OPEVAL were similar to the ones used in the first OPEVAL. In preparation for the second OPEVAL, USFK added the requirement that the data collectors at each site and personnel at an analysis cell conduct real-time data analysis. Further, USFK conducted a baseline comparison to validate that the procedures used by the data collectors were effective and a comparison of sent and received products was made to analyze the timeliness, completeness, and accuracy of the data collected.

Audit Response. The USFK comments are responsive. Requiring data collectors and analysis cell personnel to conduct real-time data analysis; conducting a baseline comparison to validate the procedures used by the data collectors; and comparing the sent and received products to analyze the timeliness, completeness, and accuracy of the data collected meets the intent of the recommendation.

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

Scope and Methodology

We reviewed and evaluated the adequacy of the contingency planning and OPEVAL reporting efforts by USFK. We also reviewed and evaluated the actions taken by USFK to coordinate with the ROK on Y2K issues concerning host nation support (see Appendix C). We met with the Y2K focal points for USFK and its subordinate commands to identify actions taken to ensure continuity of mission capability in the event of Y2K-related disruptions or failures and for compiling, evaluating, and reporting USFK OPEVAL results to the Joint Staff. We also assessed actions taken by USFK and its subordinate commands to coordinate efforts with the ROK on Y2K issues associated with the electricity, water, collocated operating bases, and the 12 wartime host nation support functional areas. We compared the actions taken by USFK since November 1998 with those described in the DoD Y2K Management Plan and the Joint Staff's Year 2000 Operational Evaluation Guide, dated April 1, 1999. We obtained the contingency plans prepared as of July 1999 and the detailed support for the reports USFK submitted to the Joint Staff on the results of its April 1999 OPEVAL. We used that information to assess the adequacy of USFK contingency planning and operational evaluation efforts.

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

> **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 21st century infrastructure. **Performance Goal 2.2:** Transform U.S. military forces for the future. **(00-DoD-2.2)**

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 objectives and goals in the Information Technology Management Functional Area:

- **Objective:** Provide services that satisfy customer information needs. **Goal:** Modernize and integrate DoD information infrastructure. **(ITM-2.2)**

- **Objective:** Provide services that satisfy customer information needs. **Goal:** Upgrade technology base. **(ITM-2.3)**

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 Management and Technology high-risk area.

Audit Type, Dates, and Standards. We performed this program audit from July to August 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 use computer-processed data for this audit.

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

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness area in the FY 1998 Annual Statement of Assurance.

Appendix B. Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at http://www.gao.gov/. Inspector General, DoD, reports can be accessed over the Internet at http://www.dodig.osd.mil/. Final reports related to our audit of "Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility" are listed below.

Inspector General, DoD

Inspector General, DoD, Report No. 00-028, "Host Nation Support to U.S. Forces in Japan," October 28, 1999.

Inspector General, DoD, Report No. 00-001, "Alaskan Command," October 1, 1999.

Inspector General, DoD, Report No. 99-254, "Operational Evaluation Planning by U.S. Forces Korea," September 16, 1999.

Inspector General, DoD, Report No. 99-245, "Operational Evaluation Planning at U.S. Pacific Command Headquarters," September 2, 1999.

Inspector General, DoD, Report No. 99-163, "Host Nation Support to U.S. Forces Korea," May 17, 1999.

Inspector General, DoD, Report No. 99-126, "Strategic Communications Organizations," April 6, 1999.

Inspector General, DoD, Report No. 99-125, "U.S. Forces Korea," April 7, 1999.

Inspector General, DoD, Report No. 99-086, "III Marine Expeditionary Force," February 22, 1999.

Inspector General, DoD, Report No. 99-085, "Hawaii Information Transfer System," February 22, 1999.

Appendix C. Host Nation Support

Inspector General, DoD, Report No. 99-163, "Host Nation Support to U.S. Forces Korea," May 17, 1999, stated that neither Y2K interface agreements nor assurances of Y2K compliance existed between ROK organizations and USFK concerning host nation support provided to U.S. forces in Korea. During this audit (Report No. D-2000-029), we assessed actions taken by USFK and its subordinate commands to coordinate efforts with the ROK on Y2K issues associated with electricity, water, collocated operating bases, and the 12 wartime host nation support functional areas.

Based on our review, we were pleased with the efforts taken by USFK. USFK made significant progress to coordinate with the ROK on Y2K issues concerning host nation support and bring about a working relationship that will facilitate the establishment of interface agreements, the necessary assurances of Y2K compliance, and a combined effort that includes the sharing of USFK Y2K information with the ROK. Specifically, we found that USFK had obtained sufficient documentation and insight into the ROK Y2K renovation efforts for the host nation support areas that we reviewed, with the exception of ammunition, petroleum, transportation, and water. USFK had made efforts in those areas but was waiting for the conclusion of efforts by the ROK. We believe, and USFK management agreed, that USFK should strive to achieve closure of those host nation support issues as soon as practicable.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Under Secretary of Defense for Personnel and Readiness
Under Secretary of Defense for Policy
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense (Command, Control, Communications, 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

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Commanding General, Eighth U.S. Army
Auditor General, Department of the Army
Chief Information Officer, Army
Inspector General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Commander, U.S. Naval Forces, Korea
Auditor General, Department of the Navy
Chief Information Officer, Navy
Inspector General, Department of the Navy

Marine Corps

Commandant of the Marine Corps
Commander, U.S. Marine Corps, Korea
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Commander, 7th Air Force
Auditor General, Department of the Air Force
Chief Information Officer, Air Force
Inspector 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. Forces Korea
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, Defense Contract Audit Agency
Director, Defense Information Systems Agency
  Commander, Defense Information Systems Agency, Korea
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
  United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Intelligence Agency
  Inspector General, Defense Intelligence Agency
Director, Defense Logistics Agency
Director, National Imagery and Mapping Agency
  Inspector General, National Imagery and Mapping Agency
Director, National Security Agency
  Inspector General, National Security Agency

Non-Defense Federal Organizations and Individuals

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

This page was left out of orignial document

U.S. Forces Korea Comments

HEADQUARTERS, UNITED STATES FORCES, KOREA
UNIT #15237
APO AP 96205-0010

REPLY TO
ATTENTION OF

FKCS-IR

07 OCT 1999

MEMORANDUM FOR Inspector General, Department of Defense, 400 Army Navy Drive, Arlington, Virginia 22202

SUBJECT: Response to the Office of the Inspector General, Department of Defense (DoDIG) Audit Report on Year 2000 Contingency Planning and Operational Evaluation Reporting by U.S. Forces Korea (Project No. 8CC-0049.09; 10 September 1999)

1. This is the U.S. Forces Korea (USFK) response to the subject audit report. Detailed comments to the DoDIG findings and recommendations are enclosed.

2. The USFK response contains corrections and clarifications on our Y2K contingency planning and operational evaluation reporting efforts which were discussed in the draft audit report. Significant progress has been made to resolve Y2K issue since the DoDIG audit team's visit in July 1999. USFK is in the process of finalizing and exercising Y2K contingency plans supporting critical missions An aggressive program is in-place, heightening awareness and assessment of resources.

3. The point of contact is Mr Kanik at DSN (315) 723-5187.

Encl
as

WILLIAM J. LENNOX, JR.
Major General, US Army
Assistant Chief of Staff, CJ3

CF:
USCINCPAC, ATTN: J053

UNITED STATES FORCES, KOREA

RESPONSE TO DRAFT DODIG AUDIT REPORT
"YEAR 2000 CONTINGENCY PLANNING AND OPERATIONAL EVALUATION REPORTING BY U.S. FORCES KOREA"
(PROJECT NO. 8CC-0049.09)

FINDING A: USFK'S YEAR 2000 CONTINGENCY PLANNING EFFORTS

DoDIG Recommendations for Corrective Action

Recommendation A.1: Recommend that the Commander in Chief, U.S. Forces Korea finalize year 2000 contingency plans that have not yet been completed for critical missions and systems.

USFK Response: Concur. USFK's Y2K Task Force policy is that Y2K Contingency Plans be completed not only for mission critical systems, but also for all USFK systems/devices. The Task Force continues to work closely with the components, staffs, and agencies to get the remaining plans completed prior to mid-November 1999.

Recommendation A.2: Recommend that the Commander in Chief, U.S. Forces Korea complete the review of the adequacy of Year 2000 contingency plans for critical missions and systems.

USFK Response: Concur. Continuous review of USFK's completed Y2K Contingency Plans remains an on-going effort. We intend to continue these reviews until H hour to ensure the plans satisfy any/all situations. In addition to exercising the plans and providing new guidance/direction, Task Force action officers conduct workshops with components and staffs to provide specific suggestions on means to improve their plans.

Recommendation A.3: Recommend that the Commander in Chief, U.S. Forces Korea complete the exercising of all year 2000 contingency plans for critical missions and systems to ensure viable plans and sufficient resources are in place to enable the successful accomplishment of U.S. Forces Korea's critical missions.

USFK Response: Concur. Components and staffs are aware of the requirement to exercise their contingency plans and are required to brief the status/results at USFK's Y2K Executive Steering Committee meetings. Additionally, the Task Force is developing a Master Event Scenario List (MESL) that will test specific responses to simulated Y2K problems as outlined in the various contingency plans. The USFK Millennium Information and Response Center (MIRC) is planning to conduct simulations of these potential Y2K problem scenarios in mid-November 1999.

Recommendation A.4: Recommend that the Commander in Chief, U.S. Forces Korea prioritize and coordinate the workarounds outlined in year 2000 contingency plans to ensure sufficient resources are in place to enable successful execution of critical missions, functions, and processes should the workarounds be employed simultaneously.

USFK Response: Concur. While the USFK Y2K Task Force reviews contingency plans for adequacy, various workarounds are also viewed for viability. While some command assets are being pre-positioned for possible contingencies, a focus in October 1999 will be on the cross leveling of common assets for use in various contingency plans. Reviews/reports to date indicate no major conflicts exist for use of limited resources. The Task Force discussed the routine communications restoral procedures and how they will be applied to potential Y2K induced outages. The restoral priority in case of major communications outages will follow the priorities identified in the CINC's Mission Essential Circuit List (MECL) that ensures the most critical warfighting missions continue.

FINDING B: USFK'S YEAR 2000 OPERATIONAL EVALUATION REPORTING

General Comments: The methodology developed by the CFC/USFK Y2K OPEVAL Staff, for evaluating each of the fifteen identified Thin Lines generally consisted of sending the functional message traffic and/or orders associated with the task. At each processing workstation along the path, the products were captured and examined for completeness, accuracy, and timeliness to accommodate assessing the thin line for degradation and potential Y2K induced degradation. Considerable planning went into preparations for the September OPEVAL to include incorporating lessons learned from the April OPEVAL to make the improvements necessary to conduct the most accurate evaluation possible.

DoDIG Recommendations for Corrective Action

Recommendation B.1. Recommend that the Commander in Chief, U.S. Forces, Korea ensure that operators and data collectors are properly trained on the implementation of data collection procedures in preparation for the second operational evaluation.

USFK Response: Concur. Based on our previously reported lessons learned from the April OPEVAL, we made major adjustments in preparation for the September OPEVAL. Changes included more detailed training for operators and data collectors that significantly improved the knowledge level of all participants through a daylong training class on the roles of each and the tasks to be performed. In addition, a detailed booklet was provided to each participant for use as an on-site reference. The Practical Exercise and rehearsal added in September also helped correct problems identified during the April OPEVAL by enabling all participants to gain a level of familiarity of their respective sites and then to send and receive products using the on-site systems which would later be used during the OPEVAL. The training and rehearsal combined to make all participants more aware of their duties, responsibilities and the importance of capturing the information in a timely fashion.

Recommendation B.2: Recommend that the Commander in Chief, U.S. Forces, Korea develop more specific data analysis procedures for conducting the second operational evaluation, to include the automated comparison of operational evaluation results with established baselines.

USFK Response: Concur in part. While the process and procedures used in the September OPEVAL for data collection and analysis were similar to those used in April, implementation was much more effective. This was primarily because of the improved training and preparation provided to operators and data collectors, and also by the addition of real time analysis by the data collectors at each site and the analysis cell added at CP Tango. The data being captured was more accurate and useful and it was being evaluated close to real time by the site data collectors and analysis cell located at CP Tango. The data collectors at each site conducted a first level analysis for accuracy and completeness after each run by comparing the baseline products with the products captured during each Y2K related run. This allowed early identification of any Y2K failure or task failure/degradation. The Data Collector recorded the results of this first level analysis on the OPEVAL Event List. The data collectors at each site also closely monitored the recording of time by the operators on the OPEVAL Event List for products sent and received. If the time did not comply with the time scheduled on the OPEVAL Event List, reason for delay was captured. In addition, the analysis cell at CP Tango had access to soft copies of all screen captures on ADOCS and GCCS, which allowed further QA/QC of screen captures. This analysis cell also received immediate reports and supporting documentation on all Y2K failures or task failures/degradation. This facilitated detailed analysis to determine the exact cause, Y2K and operational impact and required resolution. After the OPEVAL an analysis team comprised of the various data collectors and analysis cell from CP Tango was formed to do the final analysis of the OPEVAL products and data collected. During the final analysis, an additional comparison between the baseline and the first Y2K run was conducted to validate the procedures used by the data collectors at each site were effective. Additionally, a comparison of send and received products was conducted to analyze timeliness, completeness and accuracy. The detailed analysis after the OPEVAL validated the first level analysis and findings captured real time during the OPEVAL.

Additional Comments:

Page 11, Data Analysis Procedures and Methodology. We do not agree with the statement that, "USFK analysis procedures did not include comparison of the data collected with baselines, and the methodology used in identifying soft failures contained in OPEVAL messages was not effective." In April, a baseline was established for comparison to the Y2K related runs but was not used for the comparison until after the OPEVAL and resulted in the noted lack of quality to allow the desired detailed comparison. Data analysis procedures in April did not include sufficient real time analysis as the OPEVAL was occurring. As a result, much of the data collected was not complete and in the desired format to allow required detailed analysis. The need for real time analysis during the OPEVAL and better QA/QC was emphasized in the planning and execution of the September OPEVAL. Data collectors at each site compared the baseline product to the Y2K runs as the runs were completed resulting in a first level analysis that ensured appropriate data collection was occurring and ensuring any Y2K related failures or task failure/degradation was identified. As a result, all failures were identified and confirmed during the OPEVAL execution. These failures were provided to the Analysis Cell at CP Tango as discovered by phone and also by

fax. The Analysis Cell analyzed the noted failures and implemented a plan to ensure it was fully researched. In addition, the analysis cell at CP Tango had access to soft copies of all screen captures on ADOCS and GCCS, which allowed further QA/QC of screen captures for baseline, and Y2K related runs. After the OPEVAL, an additional comparison between the baseline and the first Y2K run was conducted to validate the procedures used by data collectors at each site were effective. Additionally, a comparison of send and received products was conducted to analyze timeliness, completeness and accuracy. The detailed analysis after the OPEVAL validated the first level analysis and findings captured during the OPEVAL.

Page 12. Methodology. We do not agree with the statement that, "The lack of an automated comparison tool created an environment in which soft failures could easily remain undetected." Most of our products were either soft copy "pictures" of edit screens, maps, and track symbology laid over a variety of backgrounds and shot at a variety of scales, or they were hard copy printouts. As such, the products simply did not lend themselves to automated comparisons. Use of an automated comparison tool to evaluate the remaining products (possible two of about 50 products) was considered for the September OPEVAL but abandoned when balanced against the complexity, risk to the capture process, overhead of intruding into the operational network, and limited product applicability. An automated tool could potentially aid in the speed and centralization of the data collection and analysis process, but will not necessarily detect soft failures more readily or accurately than a real time manual method of analysis which was done on-site during the September OPEVAL. Additional reasons for not using automated tools are as follows:

(1) Products can be compared manually, reliably. We chose to keep it as simple as possible.
(2) Time required to train data collectors and/or operators to use the tool would further compound a difficult training task with the limited time provided as well as opening the door for error in doing the automated comparison.
(3) Resources in the form of time and equipment increase significantly based on the number of personnel (199 personnel) and sites (11 geographically distributed sites) involved.
(4) OPEVALs worldwide have resulted in no Y2K anomalies associated with accuracy and completeness of textual messages indicating the probability is very low.
(5) Many of the textual messages sent and received in the September OPEVAL changed in format as they went from sender to receiver not allowing an automated comparison.

Audit Team Members

The Readiness and Logistics Support Directorate, Office of the Assistant Inspector General for Auditing, DoD prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to this report are listed below.

Shelton R. Young
Raymond D. Kidd
Robert M. Murrell
Patrick J. Nix
Keith A. Yancey
Diane M. Alvin
Michael J. Guagliano
Irvin P. McMasters
Lance E. Lockhart