

Audit

Report



YEAR 2000 ISSUES WITHIN THE U.S. PACIFIC COMMAND'S
AREA OF RESPONSIBILITY
U.S. FORCES KOREA

Report No. 99-125

April 7, 1999

Office of the Inspector General
Department of Defense

AQI 99-11-2139

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility - U.S. Forces Korea

B. DATE Report Downloaded From the Internet: 08/23/99

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 08/23/99

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.

19990824 131

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

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



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

April 7, 1999

MEMORANDUM FOR COMMANDANT OF THE MARINE CORPS
COMMANDER IN CHIEF, U.S. FORCES KOREA
ASSISTANT SECRETARY OF THE NAVY (FINANCIAL
MANAGEMENT AND COMPTROLLER)
ASSISTANT SECRETARY OF THE AIR FORCE (NAVY
(FINANCIAL MANAGEMENT AND COMPTROLLER)
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
DIRECTOR, DEFENSE INFORMATION SYSTEM
AGENCY

SUBJECT: Audit Report on Year 2000 Issues Within the U.S. Pacific Command's
Area of Responsibility-U.S. Forces Korea (Report No. 99-125)

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

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Commander in Chief, U.S. Forces Korea did not comment on draft Recommendation 1. Also, we did not receive comments from the Commander, U.S. Eighth Army, or the Commanding General, 7th Air Force, on draft Recommendation 2. We request comments from those commands be provided by May 7, 1999.

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) (pjnix@dodig.osd.mil). See Appendix C for the report distribution. The audit team members are listed inside the back cover.

A handwritten signature in black ink, reading "Robert J. Lieberman", is positioned above the typed name.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No.99-125
(Project No. 8CC-0049.02)

April 7, 1999

Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility

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 listing of audit projects addressing the issue, see the year 2000 webpage on the IGnet at <http://www.ignet.gov>.

Objectives. The overall audit objective was to evaluate whether DoD adequately planned for and managed year 2000 risks to avoid disruptions to the U.S. Pacific Command's mission. Specifically, we reviewed year 2000 risk assessments, contingency plans for mission critical systems, and continuity of operations plans to perform core mission requirements. The review included major DoD communications systems operating within the U.S. Pacific Command's area of responsibility.

Results. The U.S. Forces Korea made progress in addressing the Y2K problem. However, additional work must be done. U.S. Forces Korea must improve its year 2000 effort or it may be unable to fully plan its operational evaluations and, thus, will be unable to adequately assess whether its critical operational missions and functions can continue to be executed beyond year 2000. The instability of the international political situation on the Korean peninsula makes it vital for the U.S. Forces Korea to have a particularly vigorous and effective year 2000 conversion program.

Summary of Recommendations. We recommend that the Commander in Chief, U.S. Forces Korea, immediately identify and dedicate sufficient resources to its year 2000 efforts, identify the systems and interfaces that are critical to U.S. Forces Korea's core missions and functions, prioritize the fixes for U.S. Forces Korea's mission-critical systems and interfaces, and develop or obtain system and operational contingency plans.

We recommend that the Commander in Chief, U.S. Forces Korea, require the Component Commands and agencies with elements in Korea to assist in identifying the systems and interfaces that are critical to U.S. Forces Korea's core missions and functions, and give the year 2000 fixes needed by U.S. Forces Korea mission-critical systems and interfaces under their programmatic control top priority.

We also recommend that the Commander, U.S. Eighth Army; Commander, U.S. Naval Forces, Korea; Commanding General, 7th Air Force; Commander, U.S. Marine Forces, Korea; and Commander, Defense Information Systems Agency, Korea assist

the Commander in Chief, U.S. Forces Korea in identifying the systems and interfaces that are critical to U.S. Forces Korea core missions and functions, in developing or obtaining contingency plans for core U.S. Forces Korea missions areas and critical systems, and by assigning top priority to year 2000 fixes for systems under their programmatic control that are identified as U.S. Forces Korea mission critical systems.

Management Comments. A draft report was issued January 22, 1999. No management comments were received from the Commander in Chief, U.S. Forces Korea; Commander, U.S. Eighth Army; or the Commanding General, 7th Air Force. The Department of the Navy and the Defense Information Systems Agency concurred with the finding and recommendations. The Navy stated that the commanders of the U.S. Naval Forces and Marine Forces, Korea have taken appropriate steps to provide continuing support to U.S. Forces Korea in preparing for year 2000. The Defense Information Systems Agency stated that the Commander, Defense Information Systems Agency, Korea and the Defense Information Systems Agency, Pacific Area Command Field Office would continue to provide year 2000 support to U.S. Forces Korea in the areas identified. A discussion of management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Audit Response. The Department of the Navy and the Defense Information Systems Agency comments are sufficiently responsive and further details on agreed-upon actions will be developed during followup activities, so further responses to the final report from these agencies are not necessary.

We request that the Commander in Chief, U.S. Forces Korea; Commander, U.S. Eighth Army; and the Commanding General, 7th Air Force provide comments on the final report by May 7, 1999.

Table of Contents

Executive Summary	i
Introduction	
Background	1
Objectives	2
Finding	
Status of the U.S. Forces Korea Year 2000 Program	4
Appendixes	
A. Audit Process	
Scope	12
Methodology	13
Summary of Prior Coverage	13
B. Other Matters of Interest	14
C. Report Distribution	16
Management Comments	
Department of the Navy Comments	19
Defense Information Systems Agency Comments	23

Background

Executive Order No. 13073, "Year 2000 Conversion," February 4, 1998, mandates that Federal agencies do what is necessary to ensure that no critical Federal program experience disruption because of the Year 2000 (Y2K) computing problem. The Executive Order also requires that the head of each agency ensure that efforts to address the Y2K problem receive the highest priority.

The new target completion date for implementing Y2K compliant mission-critical systems is December 31, 1998. The DoD Y2K Management Plan stipulates the criteria for DoD Components to determine the appropriate Y2K phase for each system. Each phase of the management process represents a major Y2K program activity or segment. Target completion dates range from December 1996 through March 1999. Each system must meet defined exit criteria before proceeding into the next phase.

The Secretary of Defense issued the memorandum "Year 2000 Compliance," on August 7, 1998, and stated that the Y2K computing problem was a "critical national defense issue". He directed the Joint Chiefs of Staff to develop a Joint Y2K operational evaluation program and each of the Unified Commanders in Chiefs to review the status of Y2K implementation within his command and the command of subordinate components. On August 24, 1998, the Deputy Secretary of Defense directed that the Military Departments provide plans for Y2K-related end-to-end testing of their respective functional processes by November 1, 1998. Public Law 105-271, "Year 2000 Information and Readiness Act," October 19, 1998, is intended to encourage the disclosure and exchange of information about computer processing problems, solutions, test practices, test results, and related matters in connection with the transition to the Y2K.

The Joint Chiefs of Staff. The Chairman of the Joint Chiefs of Staff is the principal military advisor to the President, the Secretary of Defense, and the National Security Council. The Joint Chiefs of Staff have no executive authority to command the combatant forces. 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 land, naval, and air 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 and 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 is supported by Component commands from each Service: the U.S. Army Pacific Command, U.S. Pacific Fleet Command, Marine Forces Pacific Command, and U.S. Pacific Air Forces Command. In addition, the U.S. Pacific Command exercises combatant command over four sub-unified commands within the Pacific region. The sub-unified commands are the U.S. Forces Japan, U.S. Forces Korea (USFK), Alaskan Command, and Special Operations Command Pacific.

U.S. Forces Korea. The USFK is one of four sub-unified commands operating within the Pacific region. It was established in July 1957 as an outgrowth of the longtime U.S. security commitment to the Republic of Korea (ROK) that 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 both legal and moral sanctions. Legal obligations are based on the United Nations Security Council Resolution of 1950, which tasked the U.S. 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 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 to defeat enemy aggression. With the activation of the Combined Forces Command, USFK became the headquarters through which American combat forces would be mobilized to augment Combined Forces Command's fighting components. The 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 DoD adequately planned for and managed Y2K risks to avoid disruptions to the U.S. Pacific Command's mission. Specifically, we reviewed Y2K risk assessments, contingency plans for mission critical systems, and continuity of operations plans to perform core

mission requirements. The review included major DoD communications systems operated within the U.S. Pacific Command's area of responsibility. See Appendix A for a discussion of the audit scope, methodology, and prior audit coverage.

Status of the U.S. Forces Korea Year 2000 Program

USFK has made progress in addressing the Y2K problem. However, the level of effort within USFK and its Component commands and supporting agencies varied in scope and was still evolving as of late 1998. Further, USFK had not fully addressed the potential impact of Y2K problems on its ability to execute core missions and functions. This occurred because USFK had not:

- dedicated sufficient resources to Y2K efforts,
- adequately coordinated Y2K efforts with its Component commands and supporting agencies,
- fully identified and prioritized mission critical systems, and
- developed contingency plans for mission-critical systems and core missions and functions

Unless USFK improves its Y2K effort, USFK may be unable to fully plan operational evaluations and, thus, will be unable to adequately assess whether core missions and functions can continue to be executed beyond the critical Y2K rollover dates. The instability of the international political situation on the Korean peninsula makes it vital for the U S Forces Korea to have a particularly vigorous and effective year 2000 conversion program.

Y2K Actions

The USFK had taken positive actions to address and resolve Y2K problems, and senior management had reinforced the importance of the Y2K program throughout the command. Some of the actions included:

- establishing a Y2K Steering Committee,
- establishing the USFK Y2K Working Group to collect and analyze data, and to track Y2K compliance, and
- taking initial steps to establish a USFK Y2K Task Force.

Y2K Executive Steering Committee. The USFK Deputy Chief of Staff chairs the Y2K Executive Steering Committee, which was established in December 1997 to oversee progress, provide guidance, and make decisions concerning the joint, component, and agency Y2K efforts in Korea. Membership includes senior leaders (O-5 and above) from the functional directorates of the USFK, the components, and agencies with elements in Korea. Additionally, the

committee serves as a forum to facilitate the sharing of information, eliminate overlaps, and identify cross-functional issues or opportunities to accelerate Y2K system fixes.

Y2K Working Group. The USFK Y2K Working Group, also established in December 1997, supports the activities and deliberations of the USFK Y2K Executive Steering Committee, investigates Y2K issues, and identifies and shares corrective actions and lessons learned. The working group is comprised of representatives from the functional directorates of the USFK, the Component commands, and agencies with elements in Korea. The working group identifies, monitors, and resolves Y2K issues that directly impact USFK missions. As of November 10, 1998, the working group had identified and was monitoring the Y2K status of 7,153 systems. The USFK J6 Operations Division group representative chairs the working group.

Y2K Task Force. At the time of our visit, the USFK was in the process of forming a task force composed of operators, planners, and technical experts from across the functional staff to accelerate and narrow the focus of the USFK Y2K effort. The components and the ROK will also be represented on the task force. The task force will become the primary focal point for all facets of the USFK Y2K efforts. The task force will be lead by the USFK Deputy Chief of Staff, and focus on the Y2K WEB, operational evaluations, and contingency assessments. As of March 1999, a full-time staff had been assigned to the task force.

Y2K Program Management

The level of Y2K efforts within USFK and its subordinate organizations varied in scope and were still evolving. To address Y2K issues, USFK and its Component commands and supporting agencies have established separate Y2K programs. None of the Component command or supporting agency programs had been established in response to USFK guidance, but rather as result of guidance from their higher headquarters. All the commands established their Y2K efforts differently. Some developed formal programs with detailed plans to guide their efforts, while others developed their programs on an informal basis.

USFK lacks adequate visibility into its component and agency Y2K programs and has only begun to integrate Y2K priorities with other existing command priorities. USFK has been reluctant to devote resources to its Y2K effort, because of the limited availability of resources in Korea and the impact it would have on operational demands. However, now that Y2K has been declared a "critical national defense issue" and is receiving Joint Staff attention, USFK needs to develop a more active Y2K effort.

In addition to actions already taken, USFK needs to immediately reallocate or reprogram the resources needed to properly staff and fund a full-time Y2K effort. Should a budgetary shortfall exist, USFK should include it in budget

submissions and identify the consequences, in terms of exercises that must be cancelled and missions that can no longer be supported, should supplemental funds not be received.

Identification and Prioritization of Mission Critical Systems

The USFK has an extensive inventory of systems in use today. Y2K resolution efforts began with a thorough assessment of existing systems. USFK completed an inventory of USFK systems during the assessment phase of its Y2K program and set a goal of having all USFK systems Y2K compliant by March 1999. However, USFK may not have enough funds, skill, or time to fix or replace all of the non-Y2K compliant systems identified. Therefore, USFK needs to ensure its efforts are focused on fixing the systems and interfaces that are critical to its mission.

However, USFK had not fully identified or prioritized its mission critical systems. The USFK process for identifying and ranking systems, for the most part, had been limited to individual organizations establishing simple inventories of their applications and platforms. This occurred because a lack of coordination between USFK and its component commands and supporting agencies. Consequently, USFK is unable to determine whether Y2K funds are effectively used or programmed, identify problems requiring greater management attention, or adequately plan or conduct the USFK Y2K operational evaluation for systems critical to core mission areas.

USFK, in conjunction with its subordinate organizations, must assess the impact of systems or their interfaces potential failure (whether Y2K failures or interoperability failures resulting from Y2K fixes) on its core mission areas and processes and prioritize the fixes for its mission critical systems and interfaces to ensure those systems get done first. Further, since existing funds are required to be used to pay for Y2K compliance efforts, USFK must reallocate and reprogram USFK-wide funds for Y2K fixes based on mission criticality and prioritization. USFK should also require its subordinate organizations to place USFK mission critical systems and interfaces at the top of their prioritization lists and to reallocate and reprogram the funds needed to ensure those systems get fixed first. If shortages of funds exist, USFK and its subordinate organizations should identify the budget shortfalls and include them in budget submissions in accordance with the DoD Year 2000 Management Plan.

Contingency Planning

Contingency planning must be accomplished to lessen the impact of Y2K induced disruptions on the USFK ability to conduct its core missions and functions. Two types of contingency plans are required to mitigate the impact of Y2K problems: system contingency plans and operational contingency plans (also referred to as continuity of operation plans). System contingency plans

focus on restoring systems experiencing Y2K induced disruptions. Operational contingency plans focus on sustaining the minimum operational capabilities required to perform a mission or function without any or all mission-critical support systems. Risk assessment needs to be incorporated into the Y2K contingency planning process to identify system-related risks. Addressing those risks may include renovating or replacing a system, devising alternative work measures, or any combination of these activities.

USFK, and its subordinate organizations, had not fully addressed the potential impact of the Y2K problem on their ability to execute USFK's critical missions and functions. Specifically, the impact of the Y2K problem on USFK's core mission areas had not been fully assessed. System and operational contingency plans had not been prepared for all mission critical systems and functions. Copies of the contingency plans developed for nationally managed systems had not been obtained. Finally, alternative work measures for satisfying essential requirements to enable the continued performance of core missions should outages of key systems occur had not been developed. Additional efforts are necessary to provide sufficient assurance that USFK's ability to perform its mission will not be compromised by Y2K failures.

Using Selected Exercises for Y2K Operational Evaluations

Using selected command and joint exercises to test Y2K scenarios may assist USFK in making further progress to identify and resolve Y2K problems. Further, incorporating Y2K scenarios would provide USFK with the opportunity to identify and correct Y2K induced interoperability problems or to test alternative measures.

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 that are conducted in the first 9 months of 1999 include a simulated Y2K phase. The objective for including a simulated Y2K phase is to operationally evaluate the extent which information technology and national security systems will successfully operate during the Y2K. Information technology or national security systems may be excluded from the Y2K simulation phase of exercises if it is determined that the systems are incapable of performing reliably in a Y2K environment. However, in such cases, the excluded systems shall be replaced in accordance with the measures outlined in their Y2K contingency plans.

On August 7, 1998, the Secretary of Defense directed the Chairman of the Joint Chiefs of Staff to develop a joint Y2K operational evaluation program by October 1, 1998. In a June 8, 1998, message, in anticipation of that tasking, the Vice Chairman of the Joint Chiefs of Staff provided the combatant commands a synopsis of its operational evaluation plan, solicited their involvement, and requested input on Y2K operational evaluation opportunities. The Joint Staff intends to use the operational evaluations to demonstrate Y2K systems readiness in an integrated, operational environment. This level of

testing will identify and associate functions and processes with automated systems, and verify that the DoD's core missions can be accomplished in a Y2K environment.

Performing command and joint exercises to test Y2K interoperability of system interdependencies and interfaces may not be possible if the Services and agencies have not implemented the necessary Y2K corrections to the required systems. In such cases, contingency plans should be tested in an operational environment to help USFK assess its capability to continue operations if the systems fail because of Y2K problems.

The Joint Staff hosted a second Y2K operational evaluation conference in September 1998. The intent of the conference was to assemble unified command operators and exercise planners to discuss their respective Y2K operational evaluations in the context of critical missions and functions that must be accomplished. USFK began planning in November 1998 how it was going to incorporate Y2K operational evaluations into its command and joint exercises. However, unless USFK improves its Y2K effort, USFK may be unable to fully plan its operational evaluations and, thus, will be unable to adequately assess whether its core missions and functions can continue to be executed beyond the critical Y2K rollover dates. We will evaluate the adequacy of the USFK Y2K operational evaluation planning during the next phase of this audit.

Conclusion

USFK had made progress in addressing the Y2K problem as of late 1998. However, much additional work was needed. USFK has personnel deployed in an area of continued tensions and the limited resources available to USFK are already dedicated to ongoing daily operations. However, in light of clear guidance on Y2K priority and the DoD's requirement that existing resources be used to pay for Y2K efforts, USFK needs to adjust accordingly. Unfortunately, the lack of replies to the draft report does not allow us to update this final report to indicate to what extent a funding problem still exists as of April 1999.

At the time of our visit, USFK, in conjunction with the components and agencies with elements in Korea, still needed to identify USFK's mission-critical systems, assess the impact of those systems or their interfaces on its core missions areas and processes and prioritize the fixes for its mission critical systems and interfaces. Further, USFK and its subordinate organizations must develop systems and operational contingency plans to ensure that there are no disruptions to USFK's core missions and functions in the Y2K and beyond. The instability of the international political situation on the Korean peninsula makes it vital for the U.S. Forces Korea to have a particularly vigorous and effective year 2000 conversion program.

Recommendations, Management Comments, and Audit Response

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

- a. Identify and dedicate sufficient resources to Y2K efforts.**
- b. Identify the systems and interfaces that are critical to core USFK missions and functions.**
- c. Prioritize the fixes for USFK's mission critical systems and interfaces.**
- d. Develop or obtain system contingency plans for all mission critical systems.**
- e. Develop operational contingency plans for core missions, functions, and tasks.**
- f. Require Component commands and agencies with elements in Korea to:**
 - (1) Assist USFK in identifying the systems and interfaces that are critical to core USFK missions, functions, and tasks.**
 - (2) Assist USFK in developing or obtaining system contingency plans for USFK mission critical systems.**
 - (3) Assist USFK in developing operational contingency plans for core USFK missions, functions, and tasks.**
 - (4) Assign top priority to Y2K fixes for systems under their programmatic control that are identified as USFK mission critical systems.**

Management Comments Required. The Commander in Chief, U.S. Forces Korea did not comment on Recommendation 1. We request that the Commander in Chief, U.S. Forces Korea provide comments in response to the final report.

2. We recommend that the Commander, U.S. Eighth Army; Commander, U.S. Naval Forces, Korea; Commanding General, 7th Air Force; Commander, U.S. Marine Forces, Korea; and Commander, Defense Information Systems Agency, Korea:

- a. Assist USFK in identifying the systems and interfaces that are critical to the USFK core missions and functions.
- b. Assist USFK in developing or obtaining system contingency plans for USFK mission critical systems.
- c. Assist USFK in developing operational contingency plans for core USFK missions, functions, and tasks.
- d. Assign top priority to Y2K fixes for systems under their programmatic control that are identified as USFK mission critical systems.

Department of the Navy Comments. The Department of the Navy concurred with the finding and recommendations. The Navy stated that the Commander, U.S. Marine Forces, Korea, has taken appropriate steps to provide continuing support to United States Forces, Korea in preparing for Y2K. Also, the Commander, U.S. Naval Forces, Korea, is closely working with the United States Forces, Korea representatives to ensure all requirements are met. This includes providing a list of systems and interfaces and contingency plans critical to supporting United States Forces, Korea missions and functions.

Defense Information Systems Agency Comments. The Defense Information Systems Agency concurred with the finding and recommendations. The Defense Information Systems Agency stated that the Commander, Defense Information Systems Agency, Korea and the Defense Information Systems Agency, Pacific Area Command Field Office will continue to provide year 2000 support to United States Forces, Korea.

Audit Response. The Department of the Navy and the Defense Information Systems Agency comments are sufficiently responsive.

Management Comments Required. The U.S. Eighth Army and 7th Air Force did not comment on the recommendation. We request that they provide comments in response to the final report.

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 page on the IGnet at <http://www.ignet.gov>.

Scope

We reviewed and evaluated the steps USFK has taken to resolve its Y2K issues to avoid mission disruptions. We met with the Y2K focal points for the USFK, U.S. Eighth Army, 7th Air Force, U.S. Naval Forces-Korea, U.S. Marine Corps Forces-Korea, 1st Signal Brigade, 501st Military Intelligence Brigade, 19th Theater Army Area Command, and Defense Information Systems Agency-Korea to obtain the status of their Y2K efforts. We compared their Y2K efforts against those described in the DoD Management Plan issued by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). We obtained documentation including USFK's inventory of mission critical systems, contingency plans, and continuity of operation plans, and used the information to assess efforts to avoid undue disruption of the USFK mission.

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

Objective: Prepare now for an 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 objectives and goals.

- **Information Technology Management Functional Area.**
Objective: Become a mission partner. **Goal:** Serve mission information users as customers. (ITM-1.2)
- **Information Technology Management Functional Area.**
Objective: Provide services that satisfy customer information needs.
Goal: Modernize and integrate DoD information infrastructure. (ITM-2.2)

-
- **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 Management and Technology high-risk area.

Methodology

Audit Type, Dates, and Standards. We performed this program audit from September 1998 to January 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.

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>.

Appendix B. Other Matters of Interest

Host Nation Support

Host nation support to U.S. infrastructure within the ROK is vital to the success of any operations conducted in USFK area of responsibility. However, USFK had limited visibility of any Y2K impact on host nation support. This is a result of a combination of factors. For example, USFK and its subordinate organizations had just begun taking initial steps to ascertain whether ROK government organizations and commercially operated companies would be able to provide host nation support and public services beyond Y2K. Further, ROK government organizations and commercially operated companies have been reluctant to release information about their Y2K efforts to the USFK. USFK and subordinate organizations must ensure that any Y2K issues that might affect the ability of ROK government organizations and commercially operated companies to provide needed host nation support are identified and addressed. Starting in February 1999, we followed up on actions taken by USFK to ensure ROK government organizations and commercially operated companies will be able to provide host nation support and public services up to and beyond Y2K. A separate report is being prepared that will discuss recent progress.

Moratorium on Configuration Changes

Configuration management must be strictly enforced from now through the turn of the century, and beyond. The USFK should consider placing a freeze on changes to its systems and those of the component commands and agencies with elements in Korea. Changes should be permitted on an exception basis only. This should be done because any changes made to the architectures after being tested in simulated Y2K phases of military exercises may invalidate the test results by reversing previous fixes or by creating new problems. If changes are permitted to USFK's "thin line" architecture after it has been evaluated in a simulated Y2K environment, the modified system and the interfaces affected by the modification should be reevaluated in a simulated Y2K scenario. As of April 1999, overall DoD Y2K configuration management policy is under review by the Joint Staff and DoD Y2K office.

Bandwidth Management

Despite the best efforts of the USFK and its components to bring all systems into Y2K compliance, there will undoubtedly be some systems that experience Y2K related disruptions. Thus, this will require the users of those systems to execute the procedures outlined in their operational contingency plans and to use alternative means for maintaining continuity of operations. To some degree, that will include a number of those users transitioning to systems that remain operational, potentially creating a situation where bandwidth requirements exceed the bandwidth available. To ensure that its most critical requirements are met should that situation come to pass, USFK needs to review the operational contingency plans developed for its core missions, functions, and tasks and develop a USFK theater-level communications systems contingency plan. The plan should cross-level and prioritize users' bandwidth requirements and be used to allocate the bandwidth available on and after the Y2K.

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)
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Deputy Assistant Secretary of Defense (Command, Control, Communications, Intelligence, Surveillance, Reconnaissance, and Space Systems)
Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
Principal Deputy – Y2K
Assistant Secretary of Defense (Public Affairs)

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)
Commandant of the Marine Corps
Commander, U.S. Naval Forces, Korea

Auditor General, Department of the Navy
Chief Information Officer, Navy
Inspector General, Department of the Navy
Commanding General, U.S. Marine Corps, Korea
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Commanding General, 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. Atlantic Command
Commander in Chief, U.S. Southern Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. Space Command
Commander in Chief, U.S. Special Operations Command
Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command

Other Defense Organizations

Director, 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
 Defense Information and Financial Management Systems, Accounting and
 Information Management Division
 National Security and International Affairs Division Technical Information Center,

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 Committee on Armed Services
House Subcommittee on Defense, Committee on Appropriations
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veteran Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Committee on Science

Department of the Navy Comments



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

01 Mar 99

MEMORANDUM FOR THE DEPARTMENT OF DEFENSE ASSISTANT INSPECTOR
GENERAL FOR AUDITING

Subj: DRAFT REPORT ON THE AUDIT REPORT ON YEAR 2000 ISSUES WITHIN
THE U.S. PACIFIC COMMAND'S AREA OF RESPONSIBILITY - U.S.
FORCES KOREA (PROJECT NO. 8CC-0049.02)

Ref: (a) DODIG memo of 22 Jan 99

Encl: (1) Department of the Navy Response to Draft Audit Report

I am responding to the draft audit report forwarded by reference (a) concerning Year 2000 issues within the U.S. Pacific Command's area of responsibility - U.S. Forces Korea (project no. 8CC-0049.02).

One of the Department of the Navy's highest priorities is to ensure no mission critical system failures occur due to Year 2000 (Y2K) related problems. To address this issue, the Department has provided guidance which outlines a centralized management/decentralized execution policy. The Department's Y2K progress is reported to Senior Management during regularly scheduled briefings. These reports examine Echelon II Commands for proper allocation of resources, for progress against Department of the Navy and Department of Defense mandated milestones, for contingency plans, for responsibility assignment and identification of system interfaces, for required Memoranda of Agreement, and for use of the Department of the Navy Y2K Database.

The Department of the Navy's response is provided at enclosure (1). We concur with the finding and recommendations in the draft report. The Commanders of U.S. Naval Forces and Marine Forces, Korea take their Y2K responsibilities seriously and have taken appropriate steps to ensure that the conduct of the Command's mission will not be adversely affected by Y2K induced failures.

Subj: DRAFT REPORT ON THE AUDIT REPORT ON YEAR 2000 ISSUES WITHIN
THE U.S. PACIFIC COMMAND'S AREA OF RESPONSIBILITY - U.S.
FORCES KOREA (PROJECT NO. 8CC-0049.02)

Your findings and recommendations have been helpful in
identifying necessary changes in our approach to solving this
very important challenge. My point of contact is Ms. Mahnaz
Dean, (703) 602-6280.



D. M. Wennergren
Deputy Chief Information Officer
for Y2K and Information Assurance

Copy to:
CMC
CNO
UNSECNAV
ASN(RD&A)
Naval Inspector General
Inspector General Marine Corps
Naval Audit Service
USMC CIO
USN Y2K Project Office
NAVINGEN(02)
Office of Financial Operations (FMO-31)
USMARFORK
USNFK

Department of the Navy Response
To
DoD Draft report of January 22, 1999
On
Y2K Issues within the U.S. Pacific Command's Area of Responsibility U.S. Forces
Korea (USFK)(8CC-0049.02)

Finding:

We recommend that the Commander, U.S. Eighth Army; Commander, U.S. Naval Forces, Korea; Commanding General, 7th Air Force; Commander, U.S. Marine Forces, Korea; and Commander, Defense Information Systems Agency, Korea:

- a. Assist USFK in identifying the systems and interfaces that are critical to the USFK core missions and functions.
- b. Assist USFK in developing or obtaining system contingency plans for USFK mission critical systems.
- c. Assist USFK in developing operational contingency plans for core USFK missions, functions, and tasks.
- d. Assign top priority to Y2K fixes for systems under their programmatic control that are identified as USFK mission critical systems.

DON RESPONSE:

Commander, U.S. Marine Forces, Korea (MARFORK) Response:

- 2.a. Concur: Completed
- 2.b. Concur: Continuing project, MARFORK will continue to provide any required support to USFK.
- 2.c. Concur: Continuing project, MARFORK will continue to provide any required support to USFK.
- 2.d. Concur: Y2K has been a top priority since July 1997. All systems have been tested, and replaced or patched if not compliant. Only one compliance issue remains concerning a communications router, and steps are well underway to replace this noncompliant equipment.

MARFORK's Y2K Coordinator is Capt Edward Howell, DSN 723-7219,
howellea@marfork.usmc.mil.

Encl (1)

Commander, U.S. Naval Force, Korea (CNFK) Response:

CNFK concur with the facts, observations, conclusions and recommendations. The CNFK Y2K team is working closely with both USFK and COMSEVENTHFLT representatives to ensure all requirements are met. We are actively engaged in assisting with preparations for USFK's Y2K OPEVALs and meet at least weekly with USFK representatives. The following specific comments are provided:

- 2.a. Concur: CNFK provided USFK a list of the Navy systems and interfaces critical to supporting USFK's missions and functions. The initial list was provided 8 JAN 99. A second list, coordinated with COMSEVENTHFLT, was provided 11 FEB 99.
- 2.b. Concur: CNFK provided USFK draft copies of CNFK's communications continuity of operations plan (also called an operational contingency plan) 10 FEB 99. Final copy will be provided by 31 MAR 99.
- 2.c. Concur: CNFK is drafting continuity of operations plans for all mission critical functions, as directed by CINCPACFLT. Final copies will be provided to USFK by 31 MAR 99. Additionally, we have provided USFK other sample contingency plans and have offered to assist as required.
- 2.d. Concur: All mission critical CNFK communications systems will be Y2K compliant by 31 MAR 99.

CNFK's Y2K Coordinator is LCDR Valerie Rosengarn, DSN 723-5118, n36@seoul-cnfk.korea.army.mil.

Defense Information Systems Agency Comments



IN REPLY
REFER TO:

DEFENSE INFORMATION SYSTEMS AGENCY

701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

Inspector General (IG)

16 February 1999

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

SUBJECT: Response to DoD IG Draft Report, Year 2000 Issues
Within the U.S. Pacific Command's Area of
Responsibility, U.S. Forces Korea (Project 8CC-
0049.02)

1. The following is the Agency's response to the subject report:

Recommendation #2: ...Commander, DISA, Korea assist U. S. Forces Korea (USFK) (a) in identifying the systems and interfaces that are critical to the USFK core missions and functions, (b) in developing or obtaining contingency plans for core USFK missions area critical systems, (c) in developing operational contingency plans for core USFK missions, functions, and tasks, (d) and by assigning top priority to Y2K fixes for systems under their programmatic control that are identified as USFK mission critical systems.

Response: CONCUR. The Commander, DISA, Korea and the DISA PAC Field Office are already engaged in support of USFK in the areas identified.

2. If you have any questions, please call Ms. Stacy Miller, Audit Liaison, at (703) 607-6316.

RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

Audit Team Members

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

Paul Granetto
Robert Murrell
Patrick Nix
Young Jin
Keith Yancey
Gopal Jain
Diane Alvin
Elizabeth Ramos