12372

111112

BY THE COMPTROLLER GENERAL

Report To The Congress

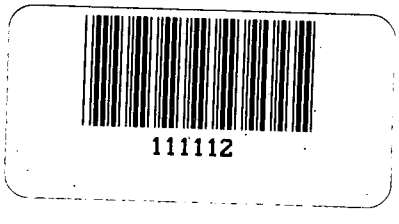
OF THE UNITED STATES

The World Wide Military Command And Control System--Major Changes Needed In Its Automated Data Processing Management And Direction

GAO's evaluation of the current World Wide Military Command and Control System ADP program showed that the problems associated with providing automated support for command and control functions, as recognized by the Department of Defense in 1966, are yet to be resolved.

The Department of Defense estimates that $1 billion has been spent on this program since 1966. The Department is currently requesting in excess of $140 million a year to continue the program.

GAO's evaluation of the program showed that the program's management structure is complex and highly fragmented which impairs the Department's ability to use sound management practices.



008088

LCD-80-22

DECEMBER 14, 1979

COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-163074

The President of the Senate and the
Speaker of the House of Representatives

This report assesses the Department of Defense's ability to resolve the problems associated with computer support of military command and control functions.

We made this review at the request of the Chairman, Subcommittee on Research and Development, House Committee on Armed Services, and Congressman Thomas J. Downey.

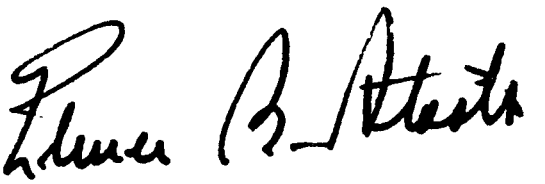
We previously reported on the issue of computer support for WWMCCS. On December 29, 1970, we reported to the Chairman, House Committee on Appropriations, on a proposed computer system acquisition to support WWMCCS and the closely related Intelligence Data Handling System. Our review of the program for the acquisition of up to 87 computers concluded that it was not adequately planned or supported by valid cost and savings estimates or determinations of need and that the responsibility for the planning and direction of the acquisition program was fragmented among several organizations.

Following our 1970 report on WWMCCS, we reported on the program to Congressman Jack Brooks on May 6, 1971 (B-163074), the Secretary of Defense on July 21, 1975 (LCD-75-116), and on April 5, 1978 (LCD-78-106), and the Congress on September 21, 1978 (LCD-78-117).

Since this report shows that many of the problems we described in our earlier reports are still present today, it is apparent that the Department has not reacted effectively to the recommendations contained in those reports.

We discussed the findings and contents of the report with officials from the Department of Defense and Honeywell Information Systems, Inc. Informal comments from the Department and Honeywell were considered in the report. Both the Department and Honeywell were given the opportunity to provide formal written comments; however, only Honeywell did so. When the Department's comments are received, we will issue a separate evaluation of the Department's and Honeywell's comments.

We are sending copies of the report to the Director, Office of Management and Budget, and the Secretary of Defense.



Comptroller General
of the United States

COMPTROLLER GENERAL'S
REPORT TO THE CONGRESS

THE WORLD WIDE MILITARY COMMAND AND CONTROL SYSTEM--MAJOR CHANGES NEEDED IN ITS AUTOMATED DATA PROCESSING MANAGEMENT AND DIRECTION

D I G E S T

The World Wide Military Command and Control System (WWMCCS) (pronounced WIMEX) is an arrangement of personnel, equipment (including automated data processing (ADP) equipment and software), communications, facilities, and procedures employed in planning, directing, coordinating, and controlling the operational activities of U.S. military forces. WWMCCS and its priority component, the National Military Command System, are essential elements of U.S. national security. WWMCCS is intended to provide the President and the Secretary of Defense a means to

--receive warning and intelligence information,

--apply the resources of the military departments,

--assign military missions, and

--provide direction to the Unified and Specified Commands.

In addition, WWMCCS is intended to support the Joint Chiefs of Staff in carrying out their responsibilities.

GAO's evaluation was directed at the WWMCCS ADP program. The WWMCCS ADP program, consisting of data communication lines, an intercomputer network, computers, and software capabilities, is an essential resource that can enable WWMCCS to achieve its intended purpose. To properly support the President, the Secretary of Defense, and the Joint Chiefs of Staff, the equipment must be compatible, data communication links must provide a direct connection (or real-time relay) whenever necessary, computerized data formats must be common, and all

LCD-80-22

components of the system configuration and operation must be as efficient as possible, both in effectiveness and in the utilization of resources.

GAO's evaluation of the WWMCCS ADP program showed that its objectives are yet to be achieved, although the Department of Defense has spent about $1 billion for this purpose since the start of the program.

Although the Department of Defense is requesting in excess of $140 million a year to continue the WWMCCS ADP program, there has been little if any, improvement realized by the Department since the program's inception. Further, GAO believes the Department of Defense's planned future expenditures to continue this program will not resolve those problems unless the Department initiates major changes in the program's management structure and direction.

GAO's evaluation showed that the existing management structure is so complex and fragmented that no one organization or individual has a complete overview of the program or the centralized responsibility for its funding, budgeting, and management. This condition impairs the Department's ability to employ sound management practices. (See ch. 3 for details.)

As a result, the WWMCCS ADP program:

--Is not responsive to national or local level requirements.

--Is not reliable.

--Lacks economical and effective growth potential.

--Cannot transfer data and information efficiently.

--Makes it extremely difficult and costly to exploit ADP technology.

--Impairs each command's operational backup capability.

--Encourages independent and decentralized software development efforts, which are still prominent in the WWMCCS ADP program. Independent software development efforts are initiated separately without sufficient consideration being given to the information requirements of other commands with which information must be exchanged.

Generally, the equipment is not installed in survivable facilities and generates excessive maintenance costs. In addition, the intercomputer network is unable to provide multilevel security. (See chs. 4, 5, and 6 for details.)

The Department of Defense recognized all of these problems in 1966. The current WWMCCS ADP program was intended to resolve them.

These problems occurred because the Department of Defense's WWMCCS ADP program specification preparation and evaluation process resulted in the selection of a computer configuration and related software that was not suited for the environment in which it was to operate. A major factor contributing to these conditions was the Department's failure to properly and clearly define the information requirements of the various commanders comprising the WWMCCS community.

Most of these problems are not new and have been previously reported to the Department of Defense, along with recommendations for correction, by GAO and various Department of Defense study groups. The recommendations in these studies have not been implemented by the Department. (See ch. 7 for details.)

During the course of this evaluation, GAO was unable to fully discharge its statutory responsibilities or be totally responsive to the requests of the Chairman, Subcommittee on Research and Development, House Committee on Armed Services, and to Congressman Thomas J. Downey. The Joint Chiefs of Staff denied complete access to pertinent documents resulting from internal surveys, reviews, draft

reports, military exercises, operational plans, and future ADP plans. (See ch. 8 for details.)

To resolve these problems and to operate a responsive, reliable, and survivable command and control system, the Secretary of Defense should give project management authority and responsibility for all WWMCCS and WWMCCS related computer-based information systems to one central organization. As the WWMCCS project manager, the designated central organization should be given the authority and responsibility for:

--Determining the information requirements of the various commands which must use and rely on WWMCCS computer-based information systems to accomplish assigned missions, including the National Military Command System.

--Preparing comprehensive long- and short-range plans for the design, development, implementation, and operation of computer-based information systems that are responsive to and reliable for the WWMCCS primary and secondary missions.

--Implementing Department of Defense Directive 7920.1 on Life Cycle Management and other sound management practices as reflected in other such directives for all WWMCCS related computer-based information systems.

--Developing and implementing a system that provides a basis for tracking actual costs incurred for designing, developing, implementing, and operating computer-based information systems in support of the WWMCCS missions.

--Simplifying the exchange of information throughout the various commands.

To encourage the Department of Defense to make the needed changes in the WWMCCS ADP program management structure and direction,

GAO recommends that the Congress consider reducing WWMCCS funding in the following manner:

--Withhold funds for completion of the study to determine the operational utility of ADP in support of WWMCCS.

--Withhold funds for the WWMCCS Intercomputer Network until the Department of Defense completes its determination of the information needed by the various commands to support their command and control functions.

--Withhold funds intended to upgrade the current WWMCCS standard computer system until the Department identifies the configuration that will replace it.

These conclusions and recommendations are more fully explained in chapter 9.

GAO discussed the findings and contents of the report with officials from the Department of Defense and Honeywell Information Systems, Inc. Informal comments from the Department of Defense and Honeywell were considered in the report. Both the Department and Honeywell were given the opportunity to provide formal written comments; however, only Honeywell did so. GAO is not including Honeywell's letter in this report because GAO plans to issue a separate evaluation of both the Honeywell and Department of Defense comments (when received).

Contents

ABBREVIATIONS

ADP	automated data processing
AUTODIN II	Automatic Digital Network II
COBOL	Common Business Oriented Language
FORTRAN	Formula Translator
GAO	General Accounting Office
GCOS	General Comprehensive Operating Supervisor
IMP	Interface Message Processor
KSOS	Kernelized Secure Operating System
PWIN	Prototype WWMCCS Intercomputer Network
WIN	WWMCCS Intercomputer Network
WWDMS	World Wide Data Management System
WWMCCS	World Wide Military Command and Control System

CHAPTER 1

WHAT IS THE WORLD WIDE MILITARY COMMAND AND CONTROL SYSTEM?

The World Wide Military Command and Control System (WWMCCS) (pronounced WIMEX) is an arrangement of personnel, equipment (including automated data processing (ADP) equipment and software), communications, facilities, and procedures employed in planning, directing, coordinating, and controlling the operational activities of U.S. military forces.

WWMCCS includes the existing command and control systems of the Unified and Specified Commands, related management information systems used by the Headquarters of the Military Departments, the command and control systems of the Headquarters of the Military Departments, the command and control systems of the Headquarters of the Service Component Commands, and the command and control support systems of Department of Defense Agencies.

WWMCCS is intended to provide the National Command Authorities (the President and the Secretary of Defense) a capability to

--receive warning and intelligence information,

--apply the resources of the military departments,

--assign military missions, and

--provide direction to the Unified and Specified Commands.

In addition, WWMCCS is intended to support the Joint Chiefs of Staff in carrying out their responsibilities.

Success of WWMCCS requires that effective coordination and liaison also be maintained with activities outside the Department of Defense. Some of these activities include the White House Situation Room, the State Department Operations Center, the Central Intelligence Agency Indications Office, the U.S. Intelligence Board National Indications Center, the U.N. Military Mission, the Office of Emergency Preparedness National Warning Center, the U.S. Coast Guard Operations Center, the Federal Aviation Administration Executive Communications Control Center, and the North Atlantic Treaty Organization.

The National Military Command System, the priority component of WWMCCS, must be capable of exchanging information

either directly or indirectly between or among these differing activities. The quick and efficient exchange of information is essential if the National Command Authorities are to make appropriate and timely responses to potential or real threats to our national security. Both the communication of warning and intelligence information from all sources and the communication of decisions and commands to our military forces require that the National Military Command System be the most responsive, reliable, and survivable system that can be provided. The ability of the National Command Authorities to make appropriate and timely responses to potential or real threats also requires that all command and control systems within the Department of Defense be configured and operated for the effective support of the National Military Command System as well as their specifically assigned missions. For these reasons, the National Military Command System is an essential element of our national security.

The complexities of efficiently and effectively exchanging information between or among these differing activities are shown in figure 1. Each organization may have differing equipment and differing levels of information. For example, tactical command and control systems will contain substantially more detailed information concerning the capabilities and deployment of our military forces than would the National Military Command System. When the National Command Authorities need more detailed information, the National Military Command System must be able to obtain it quickly and efficiently from the tactical command and control systems. To meet such requirements, equipment must be compatible, communication links must provide a direct connection or real-time relay whenever necessary, computerized data formats must be common, and all details of system configuration and operation must be as efficient as possible in terms of both effectiveness and in the utilization of resources.

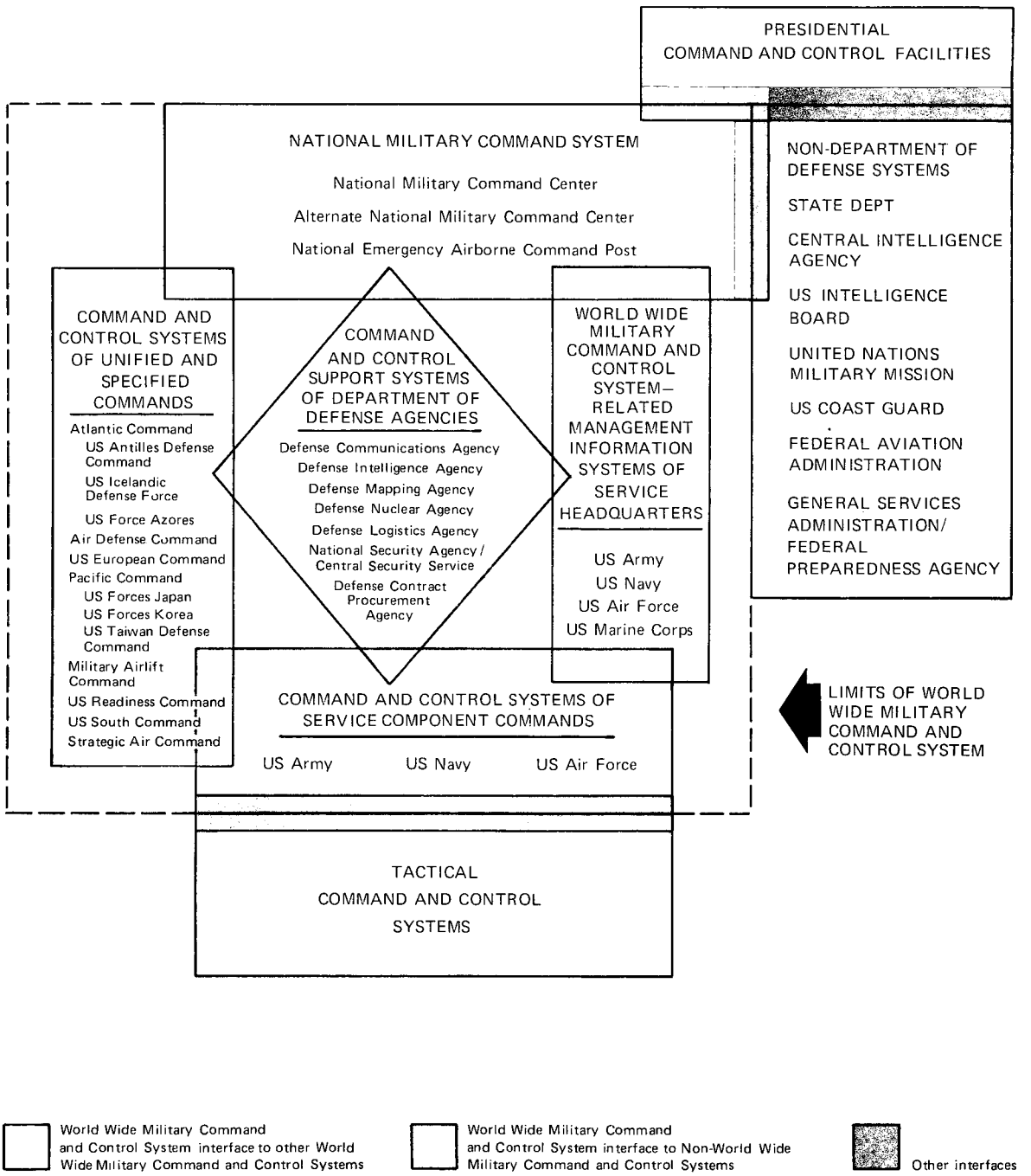
Communications and ADP capabilities are two essential resources that should enable the National Military Command System to be responsive to the National Command Authorities. We evaluated the WWMCCS ADP program, and we had previously evaluated some of the WWMCCS communication capabilities. (See app. I for a list of reports.)

EVOLUTION OF THE WWMCCS ADP PROGRAM

In the early 1960s, WWMCCS ADP capabilities consisted of a loosely knit federation of approximately 158 different computer systems, using 30 different general purpose software systems, in operation at 81 separate locations.

FIGURE 1

World Wide Military Command and Control System Relationships



These systems were unresponsive to national level requirements because they were developed separately without sufficient consideration being given to the information requirements of other commands with which they had to exchange information.

By January 1966, the Office of the Secretary of Defense and the Joint Chiefs of Staff had recognized the magnitude of these problems. As a result, they began informal discussions to improve and standardize these capabilities in support of command and control functions. A joint study group whose members represented the services, the Defense Communications Agency, and the Defense Intelligence Agency concluded that it was feasible and desirable to develop specifications to select mutually compatible computer equipment and software through industrywide competitions.

In 1969 the Office of the Secretary of Defense examined these studies, plans, and recommendations and decided to proceed with selecting standardized computers and software for use at all or some of the headquarters.

On June 4, 1970, the Deputy Secretary of Defense approved a competitive procurement of 15 to 35 standard computer systems and supporting software. The contract was awarded on October 15, 1971, to Honeywell Information Systems, Inc.

In late 1971 the Deputy Secretary of Defense recognized the need to make WWMCCS more responsive to the National Command Authorities. Department of Defense Directive 5100.30, dated December 2, 1971, established the present day WWMCCS.

The principal objective of the WWMCCS ADP program is to improve the operational effectiveness of computer equipment and software at less cost than heretofore had been possible with separate and independent equipment procurements and individual software development efforts.

SCOPE OF THE EVALUATION

On the basis of inquiries received from the Chairman, Subcommittee on Research and Development, House Committee on Armed Services, and Congressman Thomas J. Downey, we evaluated the ability of the WWMCCS ADP program to support the National Command Authorities, particularly during a time of crisis. (See apps. II and III for copies of these requests.)

While conducting this evaluation, we performed work at the following WWMCCS ADP sites and related locations:

The continental United States

The Organization of the Joint Chiefs of Staff.
National Military Command Center.
Alternate National Military Command Center.
Headquarters, U.S. Air Defense Command.
Headquarters, Strategic Air Command.
Headquarters, Military Airlift Command.
Headquarters, U.S. Army Forces Command.
Headquarters, U.S. Readiness Command.
Headquarters, Defense Communications Agency.
Headquarters, Commander-in-Chief, Atlantic.
Headquarters, Tactical Air Command.
Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

Europe

Headquarters, U.S. European Command.
Headquarters, U.S. Air Force, Europe.
Headquarters, U.S. Navy, Europe.
Headquarters, U.S. Army, Europe.
Headquarters, V Corps.
Headquarters, 8th Infantry Division.
Headquarters, 3d Armor Division.
Headquarters, VII Corps.
Headquarters, 3d Infantry Division.
Headquarters, 1st Armor Division.

Far East

Headquarters, Commander-in-Chief, Pacific.
Headquarters, Commander-in-Chief, Pacific Fleet.
Headquarters, U.S. Air Force, Pacific.
Headquarters, U.S. Forces Korea.

The major commands listed above are the principal users of WWMCCS information and have a continual need to be an interactive part of the national military command and control environment.

To the extent possible, we analyzed documents, records, reports, and related information concerning the WWMCCS ADP program. However, the Joint Chiefs of Staff restricted our access to most of the information we considered to be pertinent to our evaluation. A complete description of our access to records problem is contained in chapter 8 of this report. Restriction of access to pertinent documents has impaired our ability to be completely responsive to the congressional inquiries which initiated this evaluation.

CHAPTER 2

WHAT IS WRONG WITH THE WWMCCS ADP PROGRAM?

Our evaluation of the current WWMCCS ADP program showed that the problems associated with providing automated support for command and control functions, as recognized by the Department of Defense in 1966, are yet to be resolved and the objectives of the program are yet to be achieved. Thus, there has been little, if any, improvement realized by the Department of Defense since the inception of the program. We believe the Department's planned future expenditures to continue this program will not resolve those problems unless it initiates major changes in the program's management structure and direction.

In the early 1960s, the WWMCCS ADP structure represented a loosely knit federation of approximately 158 different computer systems.

These systems

--were not responsive to national level requirements;

--were not true systems because they were developed separately without sufficient consideration being given to the information requirements of other commands with which they had to exchange information;

--lacked growth potential;

--used incompatible hardware, software, and data base structures;

--could not transfer data and information efficiently; and

--made it extremely difficult to exploit ADP technology because of the vast differences in equipment and software systems.

In addition,

--independent or decentralized system development efforts were very costly;

--multiple equipment procurements were made at single unit prices, usually at General Services Administration contract prices instead of consolidating procurements to obtain discount prices;

--commands were forced to make an excessive number of sole source procurements to try to keep software conversion costs down; and

--commands experienced multiple (similar) software development costs, maintenance costs, and logistical support costs because equipment and software had not been standardized.

To resolve these problems, the present day WWMCCS ADP program was intended to

--make the National Military Command System the most responsive, reliable, and survivable system that can be provided with the resources available;

--centralize WWMCCS ADP management activities;

--simplify the exchange of information throughout the various commands through the use of standard equipment, a standard data base management system, standard programs, standard terminology, and standard data formats; and

--facilitate and enhance each command's operational backup capability and personnel training requirements.

We found that WWMCCS ADP capabilities are not responsive to national or local level requirements. The principal reason is that the WWMCCS standard computer system--the computers and software--basically was not designed to function in an online interactive mode as required by the command and control environment. (See chs. 4 and 5 for details.)

We also found that the program's existing management structure is so complex and fragmented that no one central organization or individual has a complete overview of the program or the centralized responsibility for its funding, budgeting, and management. This highly complex and fragmented management structure seriously impairs the Department's ability to employ sound management practices. (See ch. 3 for details.)

We further found that the exchange of information throughout the various commands has not been simplified. "Standard" WWMCCS programs do not meet the needs of local commands because they do not provide commanders the right information, at the right time, in usable formats, or in sufficient detail to make decisions. Consequently, independent software development efforts are initiated separately

without sufficient consideration being given to the information requirements of other commands with which information must be exchanged. (See ch. 5 for details.)

Finally, we found that a command's operational and backup capabilities are seriously impaired because the WWMCCS Intercomputer Network (WIN) is not reliable. This condition is partially attributable to basic design deficiencies in the standard computer system which cannot be made to function efficiently, effectively, and economically in an online interactive mode as required by the command and control environment. (See ch. 6 for details.)

Since at least 1970, we and various Department of Defense study groups have recommended ways to resolve these problems. However, the Department has not implemented these recommendations. (See ch. 7 for details.)

Because of the current status of the program and its importance to the Nation's security, major changes are required in the program's management structure and direction. These changes are sequential and interdependent in nature. For example, the Department of Defense must first centralize the program's management. Then it must determine the information requirements of the various commands that are to be interconnected by a computer network and use this information as a foundation to determine the type of equipment and software needed to make the WWMCCS ADP program responsive and reliable. Until such steps are taken, the Congress should consider reducing or eliminating further funding of the program as recommended in chapter 9.

CHAPTER 3

WHO IS IN CHARGE OF THE WWMCCS ADP PROGRAM?

One of the principal objectives of the current WWMCCS ADP program was to centralize the program's management activities. Our evaluation showed that the existing management structure is so complex and fragmented that no one organization or individual has a complete overview of the program or the centralized responsibility for its funding, budgeting, and management. This highly complex and fragmented management structure impairs the Department of Defense's ability to use sound management practices. The current management structure is also a major factor preventing it from designing, developing, implementing, and operating command and control systems which provide information when and where needed for decisionmaking.

MANY PEOPLE HAVE PARTIAL RESPONSIBILITY AND PARTIAL AUTHORITY

Department of Defense Directive 5100.30, dated December 2, 1971, divided the program's management structure among the WWMCCS Council, the Joint Chiefs of Staff, the Chairman of the Joint Chiefs of Staff, the Assistant Secretaries of Defense (Telecommunications, Intelligence, and Comptroller), and the three military services.

In essence, this directive fragmented the WWMCCS ADP program management structure in the following fashion:

--The WWMCCS Council was made responsible for providing policy guidance for the development and operation of WWMCCS.

--The Joint Chiefs of Staff was made responsible for evaluating the overall effectiveness of WWMCCS.

--The Chairman of the Joint Chiefs of Staff was made responsible for developing and validating requirements and for developing an overall WWMCCS objectives plan.

--The Assistant Secretary of Defense (Telecommunications) was given the responsibility to advise the Secretary of Defense on all matters relating to the design, development, procurement (except ADP equipment), and performance of WWMCCS.

--The Assistant Secretary of Defense (Intelligence) was given the responsibility to advise the Secretary of Defense on all matters relating to warning and intelligence.

--The Assistant Secretary of Defense (Comptroller) was made the central focal point for ADP procurements, reporting, and reutilization.

--The three military services retained the responsibility for funding and budgeting the acquisition of equipment and for developing software.

Since each of the three services is assigned different military missions and each funds and budgets its own equipment acquisitions and software development efforts, there is little incentive for them to work together cooperatively to acquire compatible and interoperable equipment and software.

A program of national importance such as WWMCCS needs a strong centralized management structure if systems are to be designed, developed, and operated within cost and budgetary limitations and provide needed information in support of the National Command Authorities. Department of Defense Directive 5100.30 did not provide this form of management structure.

On November 21, 1975, Department of Defense Directive 5100.79 further fragmented the WWMCCS ADP program management structure. The directive created the WWMCCS Engineering Organization and established the position of the WWMCCS Engineer.

The WWMCCS Engineer headed the WWMCCS Engineering Organization and was given the responsibility for performing general system engineering of WWMCCS. The WWMCCS Engineering Organization was created as a separate organizational entity of the Defense Communications Agency.

The WWMCCS Council, Chairman of the Joint Chiefs of Staff, Joint Chiefs of Staff, Assistant Secretaries of Defense, and the three military services retained the responsibilities previously assigned to them.

One of the major problems associated with this form of management structure was the fact that the Director, WWMCCS Engineering (also the Director, Defense Communications Agency), was responsible to two different organizational entities. For organizational and technical matters he was under the staff supervision of the Director, Telecommunications and Command and Control Systems (currently the Assistant Secretary of Defense, Communications, Command, Control, and Intelligence). For matters pertaining to doctrine, operational policies and procedures, development and validation of requirements, and warning and intelligence, he reported to the Chairman of the Joint Chiefs of Staff. This division of

management responsibilities seriously compounded the problems of efficiently coordinating ADP system development efforts. Moreover, the Director, WWMCCS Engineering, did not have any authority or responsibility for the overall WWMCCS ADP program funding, budgeting, and management.

The subsequent WWMCCS ADP program management structure, which had evolved since the program's inception, was even more complex and fragmented.

Within the Organization of the Joint Chiefs of Staff, the Director, J-3 (Operations), has several suborganizational units that are responsible for the WWMCCS ADP program. However, by virtue of their location within the Joint Chiefs of Staff, these units have insufficient authority to effectively control the manner in which the services use the program's resources. Each service funds and budgets the development and acquisition of equipment and software in support of its command and control functions. As a result, there is no assurance that total program funds are being efficiently spent.

On June 1, 1979, subsequent to the date of our review, the Organization of the Joint Chiefs of Staff and the Defense Communications Agency signed a Memorandum of Agreement which realigned and reassigned WWMCCS ADP management responsibilities between these two organizations. This memorandum has the effect of disestablishing the WWMCCS ADP Project Manager's Office as it then existed and realigning functional activities previously covered by the J-3 WWMCCS ADP Management Division and the J-3 Information Systems Division. Many of these functional activities were reassigned to the Command Control Technical Center, a suborganizational unit of the Defense Communications Agency. The Command, Control, and Communications Directorate, containing a command and control ADP division, is located within the Organization of the Joint Chiefs of Staff. The three military services retain the responsibility for funding and budgeting the development and acquisition of equipment and software to support their command and control functions. (See app. VI for details concerning this Memorandum of Agreement.) Since this realignment and reassignment of WWMCCS ADP responsibilities is in process, we have not attempted to evaluate the effect these changes will have on the WWMCCS ADP program.

ACCOUNTABILITY IS FRAGMENTED

The current WWMCCS ADP program management structure has not yet developed an effective mechanism for monitoring and evaluating costs. This limits its ability to respond quickly to inquiries about the system's cost and jeopardizes effective management of the program.

Virtually no cost controls are associated with the WWMCCS ADP program. The Department of Defense has estimated that $1 billion has been spent on the WWMCCS ADP program. However, the Department was unable to provide us with documentation as to the actual costs spent for the program. WWMCCS managers attributed their inability to adequately account for the money to the lack of budget authority and the numerous changes in defining the WWMCCS ADP program elements, particularly within the three military services.

We found that program costs being collected at the various sites we visited were incomplete and inconsistent. The Strategic Air Command reported the total hardware acquisition costs of two ADP systems to be $14,497,875 as of October 31, 1978. In this instance, civilian personnel salaries, wages, and fringe benefits were based on actual costs. However, military personnel costs were based on average salaries and the average number of military personnel assigned. The cost data did not include such costs as communication lines, utilities, space, training, and depreciation because these costs were not considered to be part of the WWMCCS ADP program. The Military Airlift Command spent $11.3 million to enhance its initial ADP hardware systems. In addition, the command has incurred $4.7 million in lease and maintenance charges since the systems have been installed. However, the command was unable to provide us with other operating costs for such elements as salaries, utilities, and software development.

Finally, the Department of Defense is planning to spend approximately $25 million on WIN between fiscal years 1978 and 1982. Neither Joint Chiefs of Staff nor Defense Communications Agency officials could provide documentation which supported how these figures were derived. In fact, each believed the responsibility to maintain such records belonged to the other. Despite this lack of knowledge by Department of Defense officials, we were able to determine that WIN cost figures were not all inclusive. Omitted from the figures were

--annual inflation factors,

--annual personnel costs associated with the WIN coordinator at each of the 18 sites,

--annual personnel costs of 11 civilians and 12 military personnel necessary to support the Network Operations/Technical Coordination Center, and

--costs for reliability improvements.

Without adequate cost control, it is impossible for the Department to conduct proper cost-benefit studies. A centrally administered tracking system to maintain adequate cost control is necessary if the Department is to justify additional WWMCCS computer and related equipment acquisitions and software development efforts. Such a system provides greater assurance that WWMCCS policy and operational decisions are based on the best possible information. We have previously reported 1/ that care should be taken to include all relevant costs for computer systems development and operation.

Who is in charge of the WWMCCS ADP program? No one is totally in charge or accountable for the program. Throughout the history of the WWMCCS ADP program, the management structure has been too fragmented and complex for effective program management. There was never one single organization with the responsibility, authority, and accountability for all aspects of planning, coordinating, directing, and controlling the program.

For this reason, the WWMCCS ADP program is continuing to evolve similar to the fashion of the early 1960s. A number of hardware and software systems have evolved to meet the individual needs of the Unified and Specified Commands as well as the National Command Authorities. Each military service has tended to develop these systems under its own budget and independently of other commands with which it must exchange information. Although many ongoing Defense programs affect the WWMCCS ADP program, there is no centralized long-range planning, coordination, or management and budget control over these programs. Thus, there is no assurance that annual WWMCCS ADP program costs, in excess of $140 million, are being efficiently, effectively, or economically utilized.

SOUND MANAGEMENT PRACTICES ARE NOT GENERALLY EMPLOYED IN THE WWMCCS ADP PROGRAM

The complex and fragmented management structure is a major factor contributing to the Department's inability and unwillingness to use sound management practices in the WWMCCS ADP program.

It has been a long established fact within the ADP industry and the Department of Defense that ADP systems can only be successfully and economically designed, implemented,

---

1/"Accounting for Automatic Data Processing Costs Needs Improvements" (FGMSD-78-14, Feb. 7, 1978).

and operated by passing through a series of interdependent phases. For example, Bureau of the Budget (now the Office of Management and Budget) Bulletin No. 60-6, dated March 18, 1960, provided Government-wide guidelines for initiating and conducting studies that preceded the acquisition of ADP equipment. A fundamental issue upon which long-range plans and equipment acquisitions were to be based was the clear definition of management's information requirements.

When management's information needs have been established, a determination can be made as to the availability of the source data to provide the information and, if not available, how best to make it available. As pointed out in Bulletin 60-6, only after these determinations have been made can measures be taken to determine the most appropriate system to satisfy the information needs of management. This bulletin also provided suggestions on how to identify and control costs incurred or to be incurred when developing an ADP system. Sound management practices such as those described in Bulletin 60-6 have not been used in the WWMCCS ADP program.

Another sound management practice that has not been used in the WWMCCS ADP program is life cycle management. Life cycle management is the process for administering an automated information system over its entire life with emphasis on improving early decisions which affect the system's cost and utility. The life cycle of an automated information system is composed of five broad phases: mission analysis/project initiation, concept development, definition/design, system development, and deployment/operation. The life cycle process seeks to assure management accountability for the success or failure of automated information system developments and to identify the roles and responsibilities of functional, telecommunications, and ADP managers throughout the system's life cycle. The life cycle process also seeks to

--establish a control mechanism to assure that an automated information system is developed, evaluated, and operated in an effective manner at the lowest total overall cost;

--provide visibility for all resource requirements of an automated information system and communication with the Congress early in the acquisition process for a major automated information system; and

--promote cost-effective standardization of automated information systems for use throughout the Department of Defense.

Department of Defense Directive 7920.1, dated October 17, 1978, which sets forth the Department's policy on life cycle management of automated information systems identifies the criteria to be used when designating an information system a "major automated information system." This directive provides that a system meeting any one of the following criteria shall be designated as a major automated information system:

--Has anticipated costs in excess of $100 million during the timespan from the mission analysis/project initiation phase through the extension and installation of the developed automated information system to all operating sites.

--Has estimated costs exceeding $25 million in any single year.

--Is designated as being of special interest by the Office of the Secretary of Defense.

The WWMCCS ADP program, with budget requests in excess of $140 million annually and total costs to date of about $1 billion, clearly meets the first two criteria. Any ADP program of the magnitude of WWMCCS and with the problems that have plagued the program since its inception should be subjected to the control mechanisms set forth by this directive. Such control mechanisms, which are intended to assure that automated information systems are developed, evaluated, and operated in a effective manner at the lowest total overall cost, represent sound management practices.

Although the Department's directive on life cycle management was not issued until 1978, the policies it set forth are not new and have been in effect within the Department for many years. This directive only clarified and made current what had been long established policies within the Federal Government and the Department of Defense. Irrespective of this fact, Department of Defense components responsible for implementing the policies set forth in this directive have interpreted it to exempt the WWMCCS ADP program from its accountability. The reason given was that command and control systems have unique characteristics that should be exempt from the principles of life cycle management.

THE "EVOLUTIONARY APPROACH" FURTHER IMPAIRS THE USE OF GOOD MANAGEMENT PRACTICES

A Defense Science Board Task Force, in July 1978, indicated that command and control systems should be exempt from the principles of life cycle management because of the unique

characteristics of these systems. The task force categorized these characteristics as technical, managerial, organizational, and conceptual.

Technical characteristics

The most basic technical characteristics of command and control systems are that they are highly "information rich." That is to say, the behavior of the system is highly dependent in a very complex way on the information in it and the demands put upon it. Most weapon systems by contrast have relatively simple behavior and control characteristics (although they may be highly sophisticated engineering accomplishments).

Command and control systems

--must be highly adaptable to meet the many demands a commander may place upon them in the myriad of circumstances that can arise in battle;

--must perform acceptably with imperfect information; and

--should degrade gradually, rather than fail catastrophically, under damage and stress.

Managerial characteristics

Each of these technical characteristics affects the management of command and control system development and acquisition. Management is further complicated by the need to integrate the command user's diverse needs and perspectives with the wide range of technical options presented by system engineering designers. Since neither of these groups is likely to share a common vocabulary, expertise, experience, or priorities, the management problem of achieving the required capability at a reasonable cost is difficult.

Organizational characteristics

Organizational factors add another layer of unique characteristics. Most command and control systems cut across service lines at their interface, if not in actual deployment. Key users may be military service unit commanders, Commanders-in-Chief, or the National Command Authorities. Systems typically must be interoperable with many other systems designed at different times with different emphases. Researchers, designers, and users are likely to be in different organizations and in different locations. Commands, service staffs, the Office of the Secretary of Defense, and the Joint Chiefs of Staff all have important roles in generating command and control system specifications.

Conceptual characteristics

One of the biggest problems in designing, developing, and acquiring command and control systems is the problem of deciding what the system performance criteria should be, i.e., what the system should and should not do. The absence of commonly understood concepts of command and control system performance and the existence of language barriers among technologists, policy analysts, planners, and commanders all underlie the fact that the Department of Defense lacks any useful conceptual framework for evaluating or specifying command and control systems. Terms like fail-soft, adaptability, robustness, and so forth are hard to translate into specific indices for the system designer.

For these reasons, the task force believes that command and control systems should "evolve" rather than be subject to the principles of sound management.

Most of these views are shared by other Department of Defense officials, particularly the view that the "evolutionary approach" should be used in developing command and control systems.

In our view, the technological characteristics described by the task force are not unique to command and control systems. Many information systems are "information rich" and highly dependent on the information they contain and the demands placed upon them. The banking industry contains good examples of "information rich" systems with extensive demands placed upon them. Automated military supply systems, such as the Defense Integrated Data System, the Air Force's Base Supply System, and the North American Air Defense Command's missile and satellite tracking systems are other examples of "information rich" systems with extensive and time-sensitive demands placed upon them. In each instance, these systems must perform acceptably and degrade gradually, rather than fail catastrophically, under damage or stress.

The problems confronting management regarding the complexities of integrating the commander's diverse needs are also not unique to command and control systems. Any information system intended to serve multiple users is confronted with these same issues. The integration of users' diverse needs is a problem that system designers must resolve. In a command and control environment, the designers' ability to select the optimum equipment from a wide range of technical options must be governed by the users' identification of information needs. This task, identifying basic information requirements, is yet to be accomplished in the WWMCCS ADP program. These problems are compounded by the Department's

organizational structure. Command and control systems must cut across service lines if they are to provide reliable and responsive support to the National Command Authorities. The basic problems of equipment compatibility and interoperability can only be resolved with an extensive cooperative effort between the services and the various commands. Until a more cooperative effort is initiated within the Department, the WWMCCS ADP program management structure will remain complex and fragmented.

As the task force pointed out, the biggest problem in designing, developing, and acquiring command and control systems is deciding what the systems should and should not do. This problem can only be resolved when the critical or essential elements of information needed for decisionmaking are identified and agreed upon by the Commanders-in-Chief of the Unified and Specified Commands.

Although the Department prefers to use the "evolutionary approach" to develop command and control systems, this "approach" has not been used successfully in the WWMCCS ADP program. In a command and control environment, the ability to collect, process, store, retrieve, and display information when and where needed is an essential characteristic. The ability to perform these functions efficiently rests solely on the adequacy with which the users--the battlefield commanders--have identified and validated their information requirements and assured themselves such requirements have been incorporated into the system. Since each service funds its own WWMCCS command and control system development efforts, there is little, if any, incentive for the services to work together cooperatively.

Properly used, the "evolutionary approach" to system development can be a worthwhile and useful concept because it allows military commanders to improve their command and control systems as needed. Normally, system designers incorporate this capability into any system they design because, once placed into operation, changes, modifications, and improvements constantly take place. However, as presently used in the WWMCCS ADP program, the "evolutionary approach" has impaired the employment of good system development and management practices.

We believe, therefore, that the benefits of subjecting the WWMCCS ADP program to the principles of sound management practices, such as life cycle management, substantially outweigh the disadvantages if a responsive, reliable, and survivable ADP capability is to be developed and operated within time, cost, and budgetary limitations.

The concepts of life cycle management are not new because they have been included in other Department of Defense and Government-wide directives for many years. These concepts should be applied to the WWMCCS ADP program even though, perhaps, somewhat greater flexibility may be necessary--in terms of alternatives in program planning and implementation--than would be appropriate for other systems, such as logistical, personnel, or financial systems.

CHAPTER 4

HOW RESPONSIVE, RELIABLE, AND SURVIVABLE ARE THE WWMCCS STANDARD COMPUTER SYSTEMS?

The effectiveness of WWMCCS rests upon the understanding of its concepts and objectives and its innovative support by those charged with its design and operation. Both the communication of warning and intelligence from all sources and the communication of decisions and commands to the military forces require that the National Military Command System, the priority component of WWMCCS, be the most responsive, reliable, and survivable system that can be provided with the resources available. This requires that the command and control systems of all other Department of Defense components be configured and operated for effective support of the National Miltiary Command System, as well as their specific missions. Equipment must be compatible, communciation links must provide direct connection or real-time relay whenever necessary, computerized data formats must be common, and all details of system configuration and operation must be as efficient as possible in terms of both effectiveness and in the utilization of resources. These objectives must be achieved to provide the needed flow of information among and between various commands, particularly during a time of crisis.

Our evaluation showed that the WWMCCS standard computer systems as configured by the Department of Defense, do not meet and cannot be made to meet these objectives economically, efficiently, or effectively. Specifically, our evaluation showed that in a command and control environment the WWMCCS standard computer systems

--are not responsive to national or local level requirements,

--are not reliable,

--lack economical growth potential,

--cannot transfer data and information efficiently,

--make it extremely difficult and costly to exploit ADP technology,

--impair a commander's operational backup capability,

--do not provide multilevel security, and

--generally are not installed in survivable facilities.

The principal reason for these problems is that the WWMCCS standard computer system's circuitry was not designed to operate in an online interactive mode as required in a command and control environment. The system's circuitry is designed for batch processing.

Prior to the acquisition of the present computer system, many Department of Defense officials recognized the need for a system that fully reflected the online interactive computer capabilities needed in a command and control environment.

WWMCCS STANDARD COMPUTER SYSTEMS ARE UNRESPONSIVE AND UNRELIABLE

The command and control environment places demands on the WWMCCS standard computer system's circuitry which conflict with its optimum modes of operation. The command and control environment requires a particularly demanding online interactive processing capability. The WWMCCS computer system's circuitry was designed for batch or sequence processing, and although well suited for this type of processing, it does not contain a capability to function economically, efficiently, or effectively in an online interactive mode. By the late 1960s several vendors, including Honeywell Information Systems, Inc., had marketed computer systems that were designed to operate in this fashion.

The WWMCCS computer system's operating or control software requires that a complete program be brought into memory for processing rather than only the portion of the program that is to be executed. This characteristic of the system prevents its efficient operation in an interactive mode. The system must continually exchange complete programs to process higher priority work. This exchange takes considerably more time than is required by a system whose circuitry is designed for interactive processing. As a result, the user--the commander--has substantially less processing time available to him than he needs to make decisions, particularly during a time of crisis.

To attempt to resolve this problem, the Department has conservatively estimated it spent $100 million to purchase considerable amounts of additional equipment and more than $78 million to modify the system software to function in an interactive mode. However, these efforts have not resolved the basic problem associated with the WWMCCS computer system's circuity. For example, at the National Military Command Center, the WWMCCS standard computers had to be substantially reconfigured to improve response time. In this instance, additional peripheral equipment, such as disk and tape drives, were purchased at a cost of $5.2 million. The original computer system configuration cost $4.7 million.

Thus, the cost of the additional equipment was 111 percent of the original cost of the Honeywell computer system. Although response time was slightly improved, a shortage of mainframe memory continued because the computer system must bring a complete program into memory before execution can take place.

A similar growth in costs has occurred at the Strategic Air Command and Military Airlift Command. The costs of their original computer systems--$4 million and $3.5 million, respectively--have increased to over $14 million at both commands, or a growth rate of about 250 percent.

Another example concerns the North American Air Defense Command's processing requirements and capabilities. The command is responsible for tracking missiles and satellites in space. This mission is quite time sensitive and requires an online interactive computer processing capability. Prior to the time the equipment was selected, this command objected to the procurement because it was aware that the procurement did not adequately reflect the online interactive requirement. However, the Vice Chief of Staff for the Air Force informed the command that the WWMCCS standard computer system would be used for the sake of standardization. Since that time, the North American Air Defense Command has incurred additional program costs of $100 million to overcome the standard computer system's basic circuitry problem without any significant improvement in the command's capabilities. 1/

Our evaluation showed that additional computer systems have been acquired at the other WWMCCS ADP sites to try to overcome this same problem. For example, not included in the Department's conservative estimate of $100 million for additional equipment are systems such as those developed by the Strategic Air Command and considered by the Department to be WWMCCS executive aides. Since the WWMCCS standard computer system does not provide sufficient and reliable processing capabilities, several other systems have been developed and are being maintained by individual commands to meet their needs. For example:

--An online interactive computer system, which the Department calls the Command Center Processing and Display System, uses different computers for purposes of early warning. It provides the National

---

1/"NORAD's Information Processing Improvement Program--Will it Enhance Mission Capability?" (LCD-78-117, Sept. 21, 1978).

Command Authorities with tactical warning and attack assessment information. The project manager for this system is the Strategic Air Command. Strategic Air Command officials estimated that $5.3 million has been spent on this system through fiscal year 1978. The system is presently installed in four locations--the Strategic Air Command, the North American Air Defense Command, the National Military Command Center, and the Alternate National Military Command Center.

--Computer equipment from a third vendor is used to generate the Single Integrated Operations Plan for use in case of nuclear attack. The Commander-in-Chief of the Strategic Air Command is the project manager for this system. We were informed that total program costs through calendar year 1978 were $14.3 million to develop and maintain this system.

As illustrated by these examples, the WWMCCS ADP program fails to provide for economical growth potential and makes it extremely difficult and costly to exploit ADP technology. In addition, the ADP program generates excessive maintenance costs because of the volume of equipment that has been acquired from different vendors.

WWMCCS SYSTEM SOFTWARE DOES NOT SUPPORT THE COMMAND AND CONTROL ENVIRONMENT

In WWMCCS, as in any automated processing system, there are two types of software--system software and application software. The system software enables the computer to carry out the instructions contained in the application software. System software is generally provided by the equipment vendor. Application software are the computer programs written for and by the operational users of the computer equipment. (The application software problems are discussed in ch. 5.)

Honeywell Information Systems, Inc., provided two types of system software--an operating system and a data base management system. This software is known as the General Comprehensive Operating Supervisor (GCOS) and the World Wide Data Management System (WWDMS) (pronounced WIDEMS). The commercial version of GCOS (or the operating system) has been substantially modified for use in the WWMCCS ADP program.

Neither the military version of GCOS nor WWDMS was designed and cannot be modified to operate economically, efficiently, or effectively to meet the online interactive command and control information needs of the National Command Authorities or subordinate commands. The Department

of Defense has invested more than $78 million to try to adapt, retrofit, and improve this and related software. This substantial investment has been of limited success. The problem resides in fundamental deficiencies in the military version of GCOS which WWDMS must utilize to update files and retrieve information. The military version of GCOS has not kept pace with its commercial counterpart.

GCOS does not support the command and control environment

The military version of GCOS is an efficient, single-site, batch-oriented set of software. As a batch-oriented set of software, it does not provide an efficient, effective, or economic means for processing data or information in an online interactive environment. The basic design of the operating system requires it to allocate the main memory of the WWMCCS standard computers in large blocks of characters equivalent to those contained in a complete applications program. On the average, such a block may contain 25,000 to 40,000 characters. This characteristic creates a "traffic jam" within the computer because each application program must request and be provided sufficient space in memory for the entire program rather than being allocated only the space in memory it needs to execute each set of instructions. The time required to move large blocks of characters into and out of space in main memory seriously limits the computer's processing capabilities and its responsiveness, particularly during a time of high volume use, such as a crisis. Additional memory and secondary storage are required to handle these large blocks of characters. However, the movement of so many unnecessary characters complicates the use of these computers in an internetted multisite environment. One of these complications concerns the fact that there is a physical limitation as to the amount of additional memory and secondary storage capability that can be added to the WWMCCS standard computers. To help the operation in an internetted multisite environment, the same application program must at the same time reside in the main memory of each computer. If one computer does not have sufficient main memory available when needed, data and information cannot be exchanged between the two computers. Thus, the WWMCCS standard computers complicate the synchronization of information exchange in an internetted environment and make the processing of highly priority applications difficult. (See ch. 6 for examples of the Department's experience with this software in an internetted environment.)

In contrast, other computers use smaller blocks of characters in main memory to assist operation in an internetted environment. On the average, these computers use 3,000

or 4,000 characters for a page of an application program. The use of paging allows for better utilization of main memory and facilitates multisite operations because only the needed portions of the application program are called into and used in main memory rather than the entire program. This capability allows more sites to use the computer simultaneously, thus, facilitating the internetting capability of the users. Computers using the paging technology have been commercially available from a number of vendors, including Honeywell, since the 1960s.

Department of Defense officials knew of the need for an internetting capability in the WWMCCS ADP program prior to the purchase of the WWMCCS computer systems and related software. These officials were also aware that the system would not have this capability. For example, on August 12, 1970, the Commander-in-Chief, North American Air Defense Command, informed the Chief of Staff, U.S. Air Force, that the benchmark or specification for the WWMCCS standard computers would not meet the internetting requirements of his command. On August 31, 1970, the Air Force Vice Chief of Staff advised the Commander-in-Chief that the WWMCCS standard computers and related software must be used since the North American Air Defense Command was part of WWMCCS. The WWMCCS standard computers and related software were purchased on October 15, 1971. We reported 1/ to the Congress the problems the command subsequently experienced when using this equipment and related software. Other commands, such as the Strategic Air Command, have experienced similar problems. In the Strategic Air Command, less urgent jobs are allocated main memory ahead of the most urgent ones because sufficient room exists for the less urgent jobs to be immediately placed into execution. This condition tends to impair the command's mission capabilities.

To try to resolve these problems, the Department contracted with Honeywell Information Systems, Inc., and others to modify (patch) the military version of GCOS to improve its internetting capability. Although the operating system has been modified many times since it was purchased for the WWMCCS ADP program, current exercises such as "PRIME TARGET" in 1977 showed that the modifications were not economic, efficient, or effective. (See ch. 6 for details of the impact the military version of GCOS has had on the Department's ability to design and implement WIN.)

1/"NORAD's Information Processing Improvement Program--Will it Enhance Mission Capability?" (LCD-78-117, Sept. 21, 1978).

WWDMS does not support the command and control environment

Data base management systems are very desirable for ADP systems which, like WWMCCS, have dynamic data and the need to extract selected information quickly. Data base management systems are usually characterized by the ease with which computer records can be updated and information can be extracted in meaningful displays. Compared to programming languages, such as Formula Translator (FORTRAN) and Common Business Oriented Language (COBOL), much more can be accomplished with a few program statements or directions, although the computer's execution time will increase. Some data base management systems provide an easy-to-use query language that, when compared to FORTRAN and COBOL, take much less time and skill to use. Data base management systems can greatly reduce personnel costs involved in updating files and retrieving records because skilled programmers are not usually necessary. A data base management system facilitates the sharing of data and information between two or more organizations. To function efficiently, effectively, and economically, a data base management system must use computers and system software that function in an online environment. Both of these characteristics are missing in WWMCCS since the WWMCCS standard computers and the military version of GCOS were not designed to operate in such an environment.

The initial purchase of WWMCCS standard computer systems did not specify the use of any particular data base management system, although such a system was to be provided subsequently. In March 1972 the Director, Joint Chiefs of Staff, selected the Honeywell data base management system for use in the WWMCCS ADP program. At the time of this decision, both the Joint Chiefs of Staff and Honeywell knew that the commercially available Honeywell data base management system would have to be modified for use in WWMCCS. The modified version of the Honeywell system was designated WWDMS. The commercially available Honeywell data base management system was batch-processing oriented. Thus, its use as WWDMS had to retain this architecture. The major problems with WWDMS stem from its batch-oriented architecture for use in an online interactive environment. WWMDS must rely on GCOS capabilities and is exceedingly complex to use.

GCOS is the system software through which WWDMS must gain access to needed files for updating and retrieving information. The inability of the military version of GCOS to efficiently transfer data into and out of main memory impairs WWDMS's ability to perform efficiently. Also, the WWDMS batch-oriented design requires the computer to look at many

data elements in sequence until it finds the desired one, rather than immediately selecting the desired data element without looking at any others.

In addition, WWDMS has increased rather than decreased personnel training costs. We found that WWDMS requires highly skilled programmers with special training to use it. At the various commands we visited, highly trained computer programmers were needed to interpret and prepare WWDMS queries for the WWMCCS data files. The WWDMS language is detail-oriented for the technician. Thus, WWDMS is a system designed by technicians for use by technicians and does not support the command and control environment. As a result, the system is too complex to be used by individuals without these skills and training. This condition precludes meaningful development and exploitation of available data base management capabilities.

The Department of Defense's efforts to resolve WWMCCS system software problems

Since October 15, 1971, the Department of Defense has spent more than $78 million to modify the military version of GCOS, WWDMS, and related software to function in an interactive environment. The $78 million excludes amounts spent by commands other than the Defense Communications Agency. In addition, we were informed that the original contract for the Honeywell computers included 570 staff years of effort by Honeywell for such things as system software modifications and software maintenance. Department officials were unable to identify the number of staff years or the amount of money paid to Honeywell for system software modifications because the information was included in the price of the hardware.

Honeywell Information Systems, Inc., has made major modifications to the military version of GCOS since 1971. The Department of Defense canceled the most current GCOS modification because of the technical risks involved in completing the modifications and substantial programmatic cost overruns projected by Honeywell. In addition, Honeywell made major modifications to WWDMS since 1972. The WWMCCS ADP Project Manager informed us that none of these modifications have achieved a reliable online interactive processing capability because of the problems inherent in the military version of GCOS and WWDMS basic architectures. However, some minor improvements in operations have been realized. We were also informed that most all modifications to the military version of GCOS and WWDMS are the property of Honeywell Information Systems, Inc. Thus, purchase rights to these modifications would have to be negotiated

with Honeywell for them to be used or converted for use on other computers. Since these systems are written in Honeywell's machine language, they cannot be easily converted for use on other computers. Thus, any conversion effort at best would be very costly, if at all possible.

WWMCCS STANDARD COMPUTER SYSTEMS DO NOT HAVE UNIFORM AND INDEPENDENT SOURCES OF ELECTRICAL POWER

Other WWMCCS reliability problems relate to the availability of electrical power and air-conditioning. A uniform criteria for required availability of electric power does not exist for WWMCCS ADP, reflecting a deficiency in planning. For example, the WWMCCS standard computer system that supports the National Military Command Center has electric power supplied by two independent commercial power sources providing protection from local blackouts, power-grid brownouts, and irregularities in the commerical power. This commercial power feeds motor-generator sets that provide further protection against electrical transients and power level fluctuations. The Alternate National Military Command Center is supplied by an internal, redundant generating capability. The North American Air Defense Command utilizes commercial power with a backup internal generating capacity. The Strategic Air Command utilizes commercial power and an uninterruptable power supply. The uninterruptable power supply contains a battery system which regulates voltage and maintains power for as long as 20 minutes in a blackout, then switches to backup power.

Other WWMCCS computer systems do not have the same degree of reliable sources of power.

WWMCCS STANDARD COMPUTER SYSTEMS DO NOT PROVIDE MULTILEVEL SECURITY CAPABILITIES

Multilevel computer security is intended to enable users of the system, with different levels of access to classified information, to simultaneously share the same computer equipment (timesharing) and be denied access to information for which they are not authorized and do not have a need to know. Currently, multilevel computer security is not available for any computer system, including the WWMCCS standard computer system. One reason for this situation is that the WWMCCS hardware circuitry is not designed to support multilevel computer security.

Without multilevel computer security capabilities, WWMCCS ADP sites have used several alternative approaches to the

multilevel security problem. We observed the following techniques in use at different WWMCCS sites:

--Dedicated computers and separate data bases. A separate computer was used for each security level of data being processed, and the data base for each machine required manual intervention for updating files.

--Scheduled operations (periods processing). Data from each security level may be processed at separate times, in which case, the entire computer system environment (terminals, disk packs, tapes, printer ribbons, etc.) was changed or sanitized at each change of security level.

--System-high operations. All security levels may be processed together on the same computer system provided all individuals (as well as terminal areas and communications) are cleared for the highest level of information that can be processed on the system.

These techniques are costly in terms of resources and do not provide the secure time-shared computer resources needed by the military services. While each of these techniques is effective in preventing individuals from obtaining information for which they do not have the necessary security clearance, it does not restrict access to information that they may not be authorized to have or do not have the need to know.

Two basic flaws in the WWMCCS standard system's circuitry are that it is only a two-state machine and it does not provide a hardware segmentation capability. Multilevel security can be achieved easier with a three-state machine and hardware supported segmentation.

In a three-state machine, one state is used for operating the secure or privileged commands and validating passwords and access requests. This state can be referred to as the "kernel" state.

The second state is used for resource allocation and scheduling of the jobs in the computer after they have been identified as valid jobs with valid requests for data. This second state can be called the "operating system" state.

The third state is used for running the jobs themselves and can be called the "application" or "job" state.

In the WWMCCS standard computer there is a master state and a slave state. Therefore, the master state must serve

both the most secure needs of the kernel state and the needs of the operating system state. A competent systems programmer could penetrate the computer system through the operating system state.

In addition, the WWMCCS standard computer has no hardware segmentation capability. Hardware segmentation is the dividing up of the computer memory into distinct logical areas or segments that have individual access rights. For example, certain segments can have only "read" or "write" access rights, thus providing protection from unauthorized access. Segmentation is desirable to facilitate controlled software sharing by many users. For example, standard WWMCCS software could be shared in a controlled manner if segmentation capabilities were available. For these and other reasons, the WWMCCS standard computers and software do not provide, and cannot be made to provide, the multilevel security capability required in a command and control environment.

It should be noted that Honeywell's Secure Communications Process and the Defense Advanced Research Projects Agency's Kernelized Secure Operating System (KSOS) project are not the only major efforts underway addressing the computer security issue. Other such efforts include a Kernelized VM-370 operating system and substantive research efforts by MITRE, University of California at Los Angeles, and SRI International. None of these efforts have yet been certified secure by the National Security Agency or the Department of Defense nor has a method been developed for such certification. However, the need for multilevel security in the WWMCCS ADP program is irrefutable.

WWMCCS STANDARD COMPUTER SYSTEMS ARE GENERALLY NOT SURVIVABLE

The survivability of WWMCCS standard computers, ADP, and other command and control automated systems is substantially dependent upon the facilities in which the equipment is located and the supporting utilities. If the facilities are destroyed or electric power or air-conditioning capabilities disrupted indefinitely, data processing will cease unless a backup site is available. Survivability can be assessed against two conditions: acts of nature and accidents and acts of aggression and sabotage.

Except for the National Military Command Center, none of the WWMCCS ADP sites have adequate provisions to use backup computer systems at other ADP sites should acts of nature or fire stop data processing indefinitely.

We believe greater concern should be given to potential acts of aggression or sabotage. Should the WWMCCS ADP installations be jeopardized by such threats, it is almost certainly to occur when command and control is of utmost importance just before or immediately after the initiation of conflict. Any failure may affect the ability to respond appropriately to situations which otherwise may escalate. In areas where conventional war is a possibility, additional provisions should be made to ensure continuous ADP operations by improving survivability. Supporting utilities at several WWMCCS sites are unduly vulnerable to sabotage from individuals or small groups. The Department has recognized this problem for some time, but it has failed to take meaningful action. Consequently, most WWMCCS ADP facilities cannot, under any circumstances, be considered survivable.

CHAPTER 5

DOES WWMCCS APPLICATIONS SOFTWARE SUPPORT THE COMMAND AND CONTROL ENVIRONMENT?

One of the principal objectives of the current WWMCCS ADP program was to simplify the exchange of information throughout the various commands by using standard software, standard data formats, and standard terminology.

The WWMCCS ADP program has not resolved many of the software problems associated with automated support of command and control functions. There has been little, if any, improvement in software development realized by the Department since the start of the program. Software development is still fragmented and has been unable to economically and efficiently exploit state-of-the-art ADP technology.

WWMCCS STANDARD SOFTWARE DOES NOT ADEQUATELY SUPPORT THE FUNCTIONS OF COMMAND AND CONTROL

WWMCCS application software can be grouped into three categories--WWMCCS standard software, software under consideration for designation as WWMCCS standard software, and software developed by the various commands to meet their needs because of deficiencies in WWMCCS standard software.

The advantages of standard software in a command and control environment are many and varied. First, standard software can simplify the exchange of information because the same software can be used at multiple sites, thus eliminating the need for the costly and time consuming conversion of the information before it is processed at the receiving site. Second, standard software can substantially reduce training costs because decisionmakers and technicians need not be retrained in new equipment and new software each time they transferred from one location to another. Third, software maintenance costs are minimized because once made, a modification can be easily used at every location using the standard software. Fourth, standard software can increase the overall systems operational backup capability because information processed at one location can be processed at any other location using the same software and equipment. Finally, standard software increases the systems' responsiveness because all users gain access to and retrieve information in the same manner.

At the time of our review, the Joint Chiefs of Staff had approved 16 applications as WWMCCS standard software. However, standard software is standard in name only. Although commands may elect to use these applications as they see fit, most commands use very few of them. Usually the information is too old for many users, is not sufficiently detailed for local use, does not contain the right information in the right format, and cannot be accessed in a timely manner. As a result, each command has developed a substantial number of software applications to support its command and control functions. These applications have been developed at considerable cost. In some cases, functionally redundant standard applications are maintained to support Joint Chiefs of Staff reporting requirements which create additional workloads for the computer. The elimination of multiple (similar) software development efforts was a problem the current WWMCCS ADP program was intended to resolve.

On the basis of information provided by the Joint Chiefs of Staff, only four standard applications were in use at more than half of the WWMCCS sites. Two of these four systems were for computer directed training and computer resource accounting. All of the standard applications, however, are used to support the Joint Chiefs of Staff. In our opinion, the standard applications program has been only a vehicle to share software developed for the Joint Chiefs of Staff rather than to serve the primary objectives of the WWMCCS ADP program, which are to simplify the exchange and flow of information and to reduce similar or duplicative software development and maintenance costs.

The table on page 35 shows the Joint Chiefs of Staff's figures on the number of standard software applications used at each location. On the average, a standard application was in use on about 11 systems, or less than one third of the 35 WWMCCS computer sites.

The Joint Operations Planning System, one of the most frequently used large-scale standard applications, provides planners the capability to select, analyze, and tailor force options to produce an acceptable deployment scheme.

However, the Joint Operations Planning System does not maintain current data because it is updated only at infrequent intervals (i.e., quarterly or semiannually). The System aids planners by calculating resource requirements for deployment against transportation capabilities. In a major crisis or exercise, the Joint Operations Planning System has limited value because it does not reflect currently available resources. That data is contained in another data base that

uses different and incompatible data formats (Force Status and Identity System). The Force Status and Identity System is under consideration for approval by the Joint Chiefs of Staff as a WWMCCS standard software application. The Joint Operations Planning System was largely a manual system which was converted to run on the WWMCCS standard computer system. The Joint Chiefs of Staff estimated that as of November 1978 the Joint Operations Planning System software development costs totaled $6.2 million.

We also found that several of these standard applications did not support the command and control function directly, but provided ADP training, system support, or monitoring of computer resource utilization. The remaining systems provided resources or situation monitoring and operations planning. Monitoring applications involved periodic updates to descriptive data bases while planning applications generally involved less frequent updates to the data bases.

The Joint Chiefs of Staff has estimated that total expenditures for standard applications development have been about $11 million.

Similar problems were disclosed with the software applications under consideration for approval as WWMCCS standard software.

SOFTWARE UNDER CONSIDERATION AS WWMCCS STANDARD SOFTWARE DOES NOT ADEQUATELY SUPPORT THE FUNCTIONS OF COMMAND AND CONTROL

At the time of our evaluation, the Joint Chiefs of Staff were considering approving seven applications as WWMCCS standard software. The table on page 37 shows the Joint Chiefs of Staff's figures on the number of locations using these applications.

The Force Status and Identity System is the most frequently used application for resource monitoring in WWMCCS. We found that this system was of questionable value to many commands because its data files were too old for many purposes and had questionable accuracy. Many commands were using other systems in addition to, or in place of, the partially standard Force Status System because it did not meet their needs.

The Force Status System is intended to contain time-sensitive data, but changes are made through batch processing. The Joint Chiefs of Staff require commands to report changes

WWMCCS STANDARD SOFTWARE USED AT WWMCCS ADP SITES

WWMCCS ADP SITES	WWMCCS STANDARD SOFTWARE															
	JOINT RESOURCE ASSESSMENT DATA REPORTING SYSTEM	SINGLE INTEGRATED DAMAGE ANALYSIS CAPABILITY	NUCLEAR OPERATIONS MONITORING SYSTEM	JOINT OPERATION PLANNING SYSTEM	CODE WORK NICKNAME AND EXERCISE TERM SYSTEM	RECONNAISSANCE INFORMATION SYSTEM	AIR FIELD FACILITIES FILE	COMPUTER DIRECTED TRAINING SYSTEM	SUPPORT FOR WWMCCS ACCOUNTING PROGRAM	ELECTRONIC WARFARE INFORMATION SYSTEM	NUCLEAR WEAPONS ACCOUNTING SYSTEM	RECORD ASSOCIATION SYSTEM	GEOLOCATION FILE	MAJOR ITEMS OF EQUIPMENT	GENERAL ON LINE DISPLAY SYSTEM	GREAT CIRCLE DISTANCE CALCULATOR
COMMAND AND CONTROL TECHNICAL CENTER RESTON				X				X	X		X	X			X	
ALTERNATE NATIONAL MILITARY COMMAND CENTER	X	X	X			X			X	X	X		X	X	X	
NATIONAL MILITARY COMMAND CENTER		X		X	X	X	X	X	X	X	X	X	X	X		X
ARMY OPERATIONS CENTER	X	X		X	X			X	X		X	X				
COMMANDER-IN-CHIEF EUROPE	X		X	X		X		X	X	X	X		X	X	X	
ARMY WAR COLLEGE								X								
U.S. FORCES COMMAND				X				X	X		X	X				
U.S. ARMY EUROPE				X			X		X	X	X					
MILITARY TRAFFIC MANAGEMENT COMMAND				X					X			X				X
CHIEF, NAVAL OPERATIONS	X			X					X	X		X				
U.N. COMMANDER, U.S. FORCES KOREA				X	X		X	X	X	X		X	X	X		X
COMMANDER-IN-CHIEF ATLANTIC	X	X	X	X		X		X	X	X		X	X	X	X	
COMMANDER-IN-CHIEF PACIFIC	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X
U.S. NAVY EUROPE				X				X	X	X	X	X				
COMMANDER-IN-CHIEF PACIFIC FLEET				X			X	X	X	X		X				X
NAVY COMMAND AND CONTROL SYSTEM								X								
AIR FORCE DATA SERVICE CENTER	X			X			X	X		X	X					X
AIR FORCE TRAINING COMMAND				X			X	X								X
AIR UNIVERSITY								X	X							
TACTICAL AIR COMMAND				X			X	X	X	X						X
U.S.AIR FORCE EUROPE				X			X	X		X	X					X
U.S. READINESS COMMAND	X	X		X	X		X	X	X	X			X	X	X	X
STRATEGIC AIR COMMAND	X		X	X			X	X	X	X						X
NORTH AMERICAN AIR DEFENSE COMMAND	X	X		X				X	X	X			X	X		
MILITARY AIRLIFT COMMAND				X			X	X	X							X
U.S. AIR FORCE PACIFIC	X			X				X		X						
TOTAL	11	7	5	22	5	5	12	22	20	17	11	10	8	8	6	12

WWMCCS PROPOSED STANDARD SOFTWARE USED AT WWMCCS SITES

WWMCCS ADP SITES	WWMCCS PROPOSED STANDARD SOFTWARE SYSTEMS						
	FORCE STATUS AND IDENTITY SYSTEM	NUCLEAR CAPABILITIES PLAN	U.S. BASE REQUIREMENTS OVERSEAS	GENERAL UNIFIED AMMUNITIONS REPORTING DATA SYSTEM	UNIT TYPE CODE FILE	NUCLEAR CONTINGENCY PLANNING SYSTEM	FRAGMENTATION ORDER PREPARATION
COMMAND AND CONTROL TECHNICAL CENTER RESTON							N/A
ALTERNATE NATIONAL MILITARY COMMAND CENTER	X	X	X	X	X	X	N/A
NATIONAL MILITARY COMMAND CENTER	X		X	X	X		N/A
ARMY OPERATIONS CENTER							N/A
COMMANDER-IN-CHIEF EUROPE	X	X	X	X	X	X	N/A
ARMY WAR COLLEGE							N/A
U.S. FORCES COMMAND							N/A
U.S. ARMY EUROPE	X	X	X	X			N/A
MILITARY TRAFFIC MANAGEMENT COMMAND							N/A
CHIEF, NAVAL OPERATIONS							N/A
U.N. COMMANDER, U.S. FORCES KOREA	X	X			X		N/A
COMMANDER-IN-CHIEF ATLANTIC	X		X	X	X	X	N/A
COMMANDER-IN-CHIEF PACIFIC	X	X	X	X	X	X	N/A
U.S. NAVY EUROPE	X	X	X	X			N/A
COMMANDER-IN-CHIEF PACIFIC FLEET		X					N/A
NAVY COMMAND AND CONTROL SYSTEM							N/A
AIR FORCE DATA SERVICE CENTER							N/A
AIR FORCE TRAINING COMMAND							N/A
AIR UNIVERSITY							N/A
TACTICAL AIR COMMAND							N/A
U.S.AIR FORCE EUROPE	X	X					N/A
U.S. READINESS COMMAND	X	X			X		N/A
STRATEGIC AIR COMMAND							N/A
NORTH AMERICAN AIR DEFENSE COMMAND	X	X			X		N/A
MILITARY AIRLIFT COMMAND	X						N/A
U.S. AIR FORCE PACIFIC	X	X					N/A
TOTAL	13	11	7	7	8	4	

N/A = DATA NOT AVAILABLE FROM INFORMATION PROVIDED.

daily on their status of forces. The system update begins processing at the Alternate National Military Command Center at about 5 p.m. eastern standard time. However, actual changes may have occurred as much as or more than 24 hours earlier. Therefore, the timeliness of the system files maintained for the National Command Authorities' use can generally be characterized as 12 to 36 hours old. At each subordinate command, more current information is available. Current information is essential for the National Command Authorities to make proper responses in a time of crisis.

The Joint Chiefs of Staff's Force Status data base is so voluminous, with over 400,000 records, it is impractical for general use in running retrievals. As a result, the Joint Chiefs of Staff have developed a Force Status strip file with about 70,000 records against which it runs about 95 percent of its retrievals. At the commands, which use the standard Force Status, the average file size is only about 40,000 records. Although these local Force Status data bases are not large by ADP standards, they are too large in the sense that the percentage of frequently used data is very low in comparison to overall file size. This affects the data base management activities of sites by tying up more storage and processing resources than necessary, given the utility of the local Force Status and Identity Report System files.

The Joint Chiefs of Staff's Force Status file, as well as local Force Status files at several of the commands we visited, appear to have data reliability problems. The Department has not identified the extent of the problems. Various studies have commented on data reliability problems, but they have not determined the exact impact of weak controls on reporting.

The Force Status software checks each transaction to ensure that changes are reported in valid formats. About 2 percent of the transactions are rejected for invalid formats, usually due to keypunch and transmission errors, and returned to the originating command. We were informed that no other computer edit checks were employed. After the files are updated, Joint Chiefs of Staff personnel manually scan hard copy dumps of the files two to three times a week for obvious gross inaccuracies and make logic checks on the files four times a year. We were informed that there were no other controls or checks on data accuracy and there was no attempt to measure the accuracy of the data in the files or the accuracy of the reports submitted by the commands.

The Air Force Audit Agency reported problems with the accuracy of Force Status in June 1978. The report stated that

units of all eight major commands included in the audit reported changes only 6 days a week, instead of 7 days a week as required by the Joint Chiefs of Staff. Combat readiness status was incorrectly reported at 47 percent of the units. Reports of available personnel were overstated by as much as 24 percent. For 42 percent of the units, inaccurate data was reported for a variety of data elements because of weak local procedures for ensuring its accuracy. Old and inaccurate data impairs the ability of the National Command Authorities and subordinate commanders to be fully cognizant of the readiness posture of our military forces at any given point in time.

To try to develop the automated support the various commands need for the purposes of command and control and to overcome the problems associated with WWMCCS standard software and software under consideration as WWMCCS standard, each command has initiated the development of command and control software. These software developments are initiated independently of the information needs of other commands with which they must exchange information.

COMMANDERS DEVELOP THEIR OWN AUTOMATED SUPPORT FOR THE FUNCTIONS OF COMMAND AND CONTROL

The Defense Audit Service estimated that locally developed software applications cost about $40 million annually. The objectives of the WWMCCS ADP program have not been achieved because useful standard applications have not been developed and used by all commands.

One of the objectives of the standard WWMCCS ADP program was to reduce cost by providing standard system software. However, at several commands we visited, earlier practices of local and duplicative system software development and use had continued since the start of the WWMCCS ADP program. This development was necessary because the WWMCCS standard software did not meet the immediate needs of individual commands.

Several unique file access facilities have been implemented or are in final planning stages. Some examples and locations are listed below:

--Force Management Information System (Strategic Air Command).

--Storage and Retrieval System (Military Airlift Command).

--MAC Integrated Management System (Military Airlift Command).

--INQUEST (Military Airlift Command).

--TAC Automated Planning System (Tactical Air Command).

--SCN5 (U.S. Army Forces Command).

--Data Management System (Commander-in-Chief, Pacific Fleet).

Most locally developed file access systems were first implemented after the changeover to the standard WWMCCS ADP program. For example, although planning was well along prior to standardization, the Military Airlift Command analysis suggested that WWDMS would be less than satisfactory. An Air Force system which was less costly was implemented, in part, because it used significantly less main memory.

The Military Airlift Command also supplemented the military version of the GCOS operating system with a Real-time Operating System approved by the Joint Chiefs of Staff. This operating system supports the Military Airlift Command's Storage and Retrieval System. Development costs for individual system software components were not available. The Strategic Air Command also developed a supplement to the military version of the GCOS operating system--the Strategic Air Command Online Interactive Controller--which could be used simultaneously with the military version of GCOS. However, these attempts to overcome problems inherent in GCOS and WWDMS are not efficient, effective, or economical.

Where local system software is dependent upon the military version of GCOS, compatibility problems could occur with new versions of GCOS and WWDMS. There is no assurance that substantial changes made in standard software by Honeywell Information Systems, Inc., will be compatible with these other locally developed applications because the changes are contracted for the Government independent of the various software systems used locally.

The Navy is developing a new fleet command and control system used by all fleet command centers. This system will use new non-WWMCCS standard computers. The justification given for the procurement was that the WWMCCS standard computer system did not provide the needed interactive processing capabilities. The Navy estimates that procurement and maintenance costs will total several million dollars annually.

The U.S. Readiness Command has developed a software system called the Deployment Management System to meet the need of a coordinated package for planning which includes resource monitoring information. In developing this system, the Readiness Command extracted those elements of data critical to its mission from the Force Status and Joint Operations Planning data bases. The resource monitoring data in the Deployment Management System is maintained on a current basis. At other commands, users cited a need for systems similar to the Deployment Management System because the Joint Operations Planning System was inadequate for planning in a dynamic environment, such as an exercise or crisis.

Computer accounting records were not available at every site to determine computer resource utilization. However, where we were able to obtain this information, we found that locally developed command and control applications consumed much more computer resources than did standard applications, although standard applications are and should be expected to utilize the bulk of these resources if they properly supported the commander's information needs. The following table illustrates this condition:

Percentage of Computer Resources Used for Standard and Local Command and Control Applications

Location	Percent utilization for standard applications	Percent utilization for local applications
Commander, U.S. Forces Korea	23	77
Strategic Air Command		
Batch	2	98
Terminal connect hours	6	94
Military Airlift Command	2	98
Pacific Command	41	59
U.S. Army Forces Command	44	56

Local commanders have developed their own automated support for the functions of command and control since WWMCCS standard software does not meet their needs. These software development efforts are similar and very costly to develop and operate. In addition, locally developed software applications impair the command's ability to exchange information because they are developed independently without sufficient consideration being given to the information requirements of other commands with which information must be exchanged. The current WWMCCS ADP program was intended to resolve this problem.

CHAPTER 6

IS WIN RESPONSIVE AND RELIABLE?

On September 7, 1971, the Joint Chiefs of Staff recognized a need for a faster and more accurate flow of information to respond to the requirements of the National Command Authorities and subordinate commanders. A faster and more accurate flow of information is needed to ensure that the functional tasks of command and control are met, particularly during a time of crisis.

The ability to acquire, transmit, process, store, retrieve, and display the data and information needed to keep the National Command Authorities and subordinate commanders informed is heavily dependent on a responsive, reliable, secure, and survivable intercomputer network. For this reason, the Joint Chiefs of Staff subsequently directed the Defense Communications Agency to prepare plans for the design and development of the Prototype WWMCCS Intercomputer Network (PWIN).

PWIN

PWIN was intended to provide the National Command Authorities, the Joint Chiefs of Staff, and subordinate commanders a capability for direct computer-to-computer or remote terminal-to-computer exchange of information using distributed data base concepts and workload sharing techniques in a secure environment. As part of PWIN, the hardware, software, and related procedures were to be developed and tested to demonstrate the network's technical proficiency and reliability.

Under PWIN, each WWMCCS computer is connected to a Honeywell minicomputer called an Interface Message Processor (IMP). Each IMP in turn is interconnected to all of the other IMPs in the network by 50 kbps 1/ leased commerical circuits. The PWIN communications subsystem is link-encrypted for security, using KG-34 cryptographic equipment.

1/Kilobits per second (kbps) is defined as the ability to transfer one thousand binary digits of information per second from one point to another. In WWMCCS, a character consists of six binary digits, while in many commerical systems a character consists of eight binary digits known as a byte. In WWMCCS or commerical systems, a character may be an alphabetical letter, a number, or a special character, such as a period or a comma.

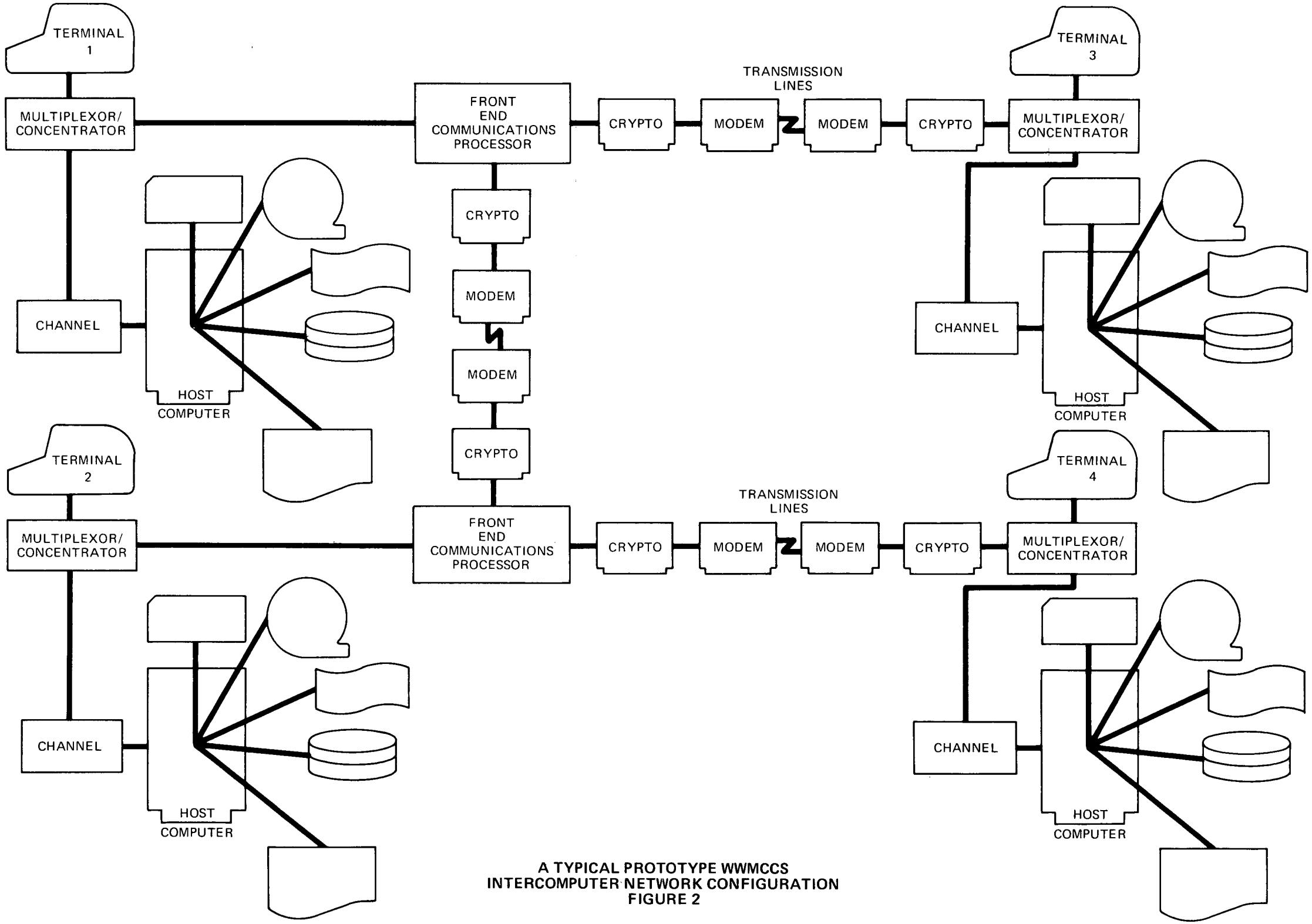
The connection between the host WWMCCS computer and the IMP is through the WWMCCS standard DATANET-355 communications processor.

Although PWIN presently uses dedicated communication lines, the eventual goal is to achieve compatibility with defense common-user communications facilities through the Automatic Digital Network II (AUTODIN II). The Defense Communications Agency is developing AUTODIN II to provide a common-user communications network to fulfill the Department's communications requirements for the 1978-85 time period. AUTODIN II is planned to provide secure delivery of data anticipated in the Department's teleprocessing operations along with a variety of additional capabilities.

PWIN was initially comprised of three interconnected WWMCCS computers located at the Command and Control Technical Center in Reston, Virginia; the National Military Command Center in the Pentagon; and the Atlantic Command in Norfolk, Virginia. As PWIN developed, it was determined that more productive experiments would be feasible if the network was expanded to include additional WWMCCS sites critical to large-scale crisis management.

On December 4, 1974, the Deputy Secretary of Defense approved the expansion to include the Alternate National Military Command Center at Fort Ritchie, Maryland; the Military Airlift Command at Scott Air Force Base, Illinois; and the U.S. Readiness Command at MacDill Air Force Base, Florida. By July 1976 the Tactical Air Command at Langley Air Force Base, Virginia; U.S. Army Forces Command at Fort McPherson, Georgia; and the services headquarters in the Pentagon were also added to the network.

PWIN is substantially more complex than the typical data communications network because a terminal cannot talk directly to another terminal. A terminal talks to a WWMCCS or host computer system which in turn talks to one or more additional computers before talking to a second terminal. This complexity adversely affects network performance and reliability because the host computer must perform additional communications functions. As explained in chapter 4, the WWMCCS or host computer system is not designed to perform such functions. Normally, communications processors perform these functions. This complex communications network is further compounded by the need to code and decode the information due to its political, economic, and military sensitivity. This complex network configuration is diagramed in figure 2 on page 45.



A TYPICAL PROTOTYPE WWMCCS INTERCOMPUTER NETWORK CONFIGURATION
FIGURE 2

This configuration will become even more complex in the 1980s when additional WWMCCS sites are added to the configuration. (See figure 3 on p. 49 for a diagram of this planned configuration.)

In addition to this complex arrangement of equipment, several different types of software are needed to make the equipment perform. In PWIN, the following types of software are used for this purpose:

--Host Computer:

  --General Comprehensive Operating Supervisor.

  --General Remote Terminal System.

  --Network Control Program.

--Multiplexor/Concentrator:

  --Data Communications Control.

--Front-End Communications Processor:

  --Intermessage Processor (switching, routing, and control).

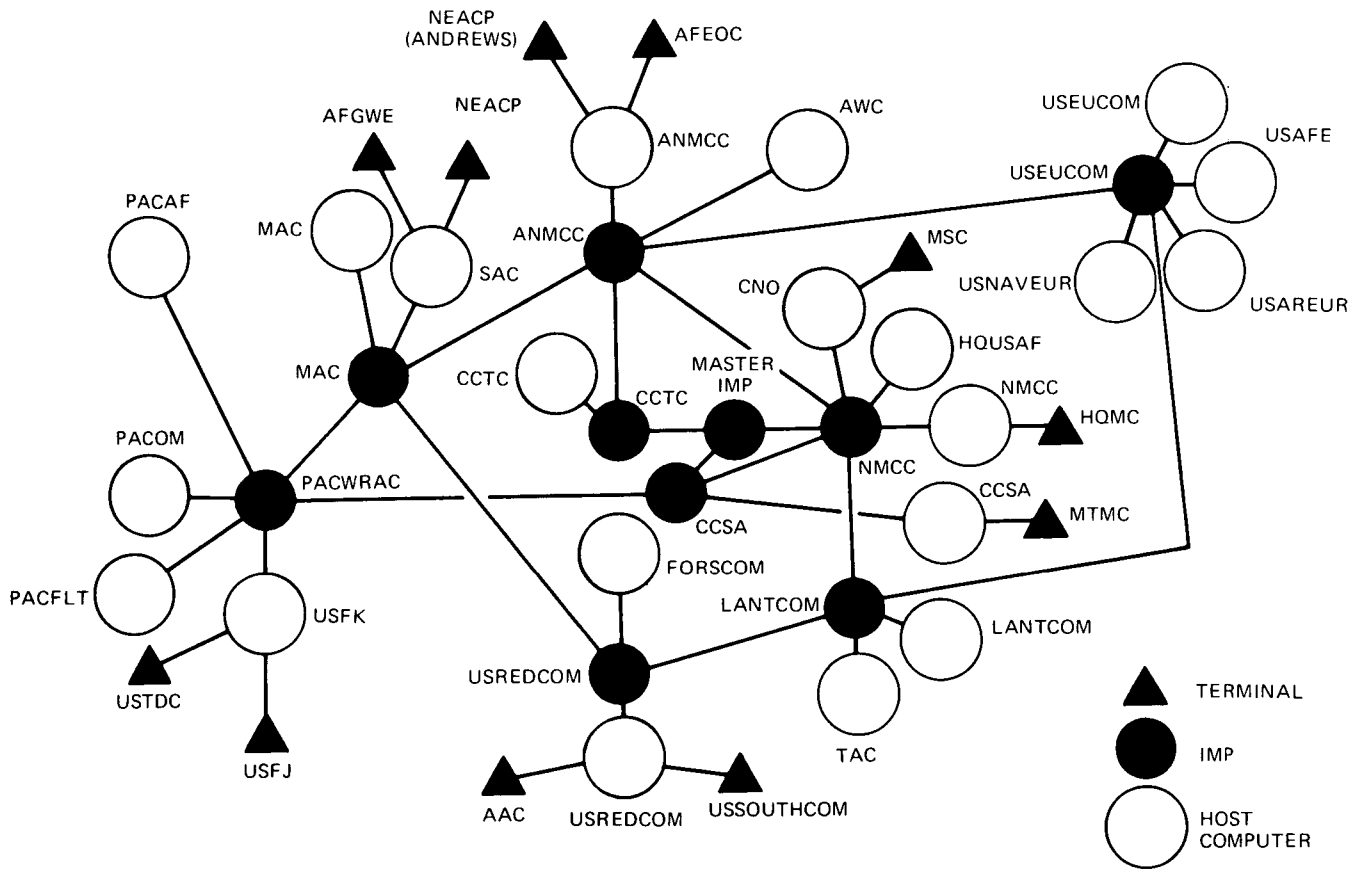
Because of this complex configuration of equipment and software, reliability of PWIN has been a problem almost since its inception. For example, on September 4, 1973, the PWIN Test Director alerted Defense Communications Agency management to the possibility that PWIN could fail. When the first comprehensive test plan for PWIN was prepared and approved on October 29, 1973, the plan emphasized that reliability could be a major problem. Obviously, the more components there are in any network, the more risk there is of any one component failing. There is no question that PWIN must be reliable if it is to be responsive to the National Command Authorities and subordinate commanders.

OPERATIONAL TESTS DISCLOSE SERIOUS PWIN RELIABILITY PROBLEMS

The Joint Chiefs of Staff tested PWIN in September and October 1976 as part of the PWIN Operational Experiment Program. The purpose of the operational tests was to analyze and evaluate the reliability and operational utility of PWIN. These tests had been delayed for several months for the following reasons:

FIGURE 3

PLANNED WIN CONFIGURATION AS OF OCTOBER 1, 1980



AAC	Alaskan Air Command	Anchorage, Alaska
AFEOC	U.S. Air Force Emergency Operations Center	Ft. Richie, Maryland
AFGWE	U.S. Air Force Global Weather Central	Omaha, Nebraska
ANMCC	Alternate National Military Command Center	Ft. Richie, Maryland
AWC	U.S. Army War College	Carlisle, Pennsylvania
CCSA	U. S. Army Command and Control Support Agency	Washington, D.C.
CCTC	Command And Control Technical Center	Reston, Virginia
CNO	Chief Naval Operations	Washington, D. C.
FORSCOM	U.S. Army Forces Command	Ft. McPherson, Georgia (Computer site at Ft. Gillem, Georgia)
HQMC	Headquarters U.S. Marine Corps.	Washington, D.C.
HQUSAF	Headquarters, U.S. Air Force	Washington, D.C.
LANTCOM	Atlantic Command	Norfolk, Virginia
MAC	Military Airlift Command	Shiloh, Illinois
MSC	Military Sealift Command	Washington, D.C.
MTMC	Military Traffic Management Command	Falls Church, Virginia
NEACP	National Emergency Airborne Command Post	Camp Springs, Maryland
NMCC	National Military Command Center	Washington, D.C.
PACAF	U.S. Air Force, Pacific	Oahu, Hawaii
PACFLT	U.S. Pacific Fleet	Oahu, Hawaii
PACOM	Pacific Command	Oahu, Hawaii
PACWRAC	PACOM WWMCCS Regional ADP Center	Oahu, Hawaii
SAC	Strategic Air Command	Omaha, Nebraska
TAC	Tactical Air Command	Hampton, Virginia
USAFE	U.S. Air Force, Europe	Ramstein, Germany
USAREUR	U.S. Army, Europe	Heidelberg, Germany
USEUCOM	U.S. European Command	Vaihingen, Germany
USFK	U.S. Forces, Korea	Seoul, Korea (Computer site at Taegu, Korea)
USFJ	U.S. Forces, Japan	Yokota Air Base, Japan
USNAVEUR	U.S. Navy, Europe	London, England
USREDCOM	U.S. Readiness Command	Tampa, Florida
USSOUTHCOM	U.S. Southern Command	Quarry Heights, Canal Zone
USTDC	U.S. Taiwan Defense Command	Taiwan
IMP	Interface Message Processor	

--Communication links between PWIN nodes were unstable.

--Communication fault corrections were uncoordinated.

--Intermessage processor and host computer/software experienced failures. These failures were due to loss of power, air-conditioning, and component failures.

The results of these tests disclosed serious problems in PWIN's reliability, bulk data file transfer capability, and computer security procedures. Most of these problems were attributable to the existing WWMCCS ADP systems and operating procedures. For example, guidance provided by the Joint Chiefs of Staff showed that PWIN must be capable of transferring information from WWMCCS standard systems, such as the Joint Operational Planning System, and from systems under consideration as WWMCCS standard, such as the Force Status and Identity System. PWIN operational tests showed that PWIN was unable to successfully transfer information from these data bases from one computer to another.

The capabilities of PWIN were again tested from March 1 through March 16, 1977, in the exercise "PRIME TARGET 77." Our review of this exercise indicated that PWIN users experienced a very large percentage of abnormal or unexpected terminations at four of the six participating sites. An abnormal termination can be defined as a termination of operations due to software or hardware or a combination of software/hardware failures.

The following table shows the experience of four participating sites. A "log on" represents an attempt to use the system.

PWIN sites	No. of log ons	No. of abnormal terminations	Percent
Atlantic Command	295	132	45
European Command	124	54	44
Readiness Command	290	247	85
Tactical Air Command	63	44	70
Command and Control Technical Center	(a)	(a)	(a)
National Military Command	(a)	(a)	(a)
Total	772	477	62

a/Not available because statistics were not developed for these sites.

Other PRIME TARGET 77 conclusions were:

--The average daily length of total PWIN outages, by line, was greater than that experienced in 1976.

--Teleconferencing was the primary mode of PWIN use in both number of users and in total time.

--Users of the system perceived a decrease in PWIN's reliability.

In their comments on the exercise, many users indicated dissatisfaction with the reliability of PWIN. One concern was that if one key site was down, the entire system went down.

THE TRANSITION FROM PWIN TO WIN

On July 18, 1977, subsequent to exercise PRIME TARGET 77 and before PWIN's unsatisfactory reliability was known, the Joint Chiefs of Staff approved the operational requirements of PWIN and authorized it to be extended to other WWMCCS sites and become an operational system called WIN. Later, when the results of the reliability study were known, the Joint Chiefs of Staff directed the Defense Communications Agency to conduct studies to

--identify problem areas which reduced the reliability of the existing network;

--identify methods for providing alternative access to the network;

--address hardware, software, communications, and procedural aspects which contributed to network reliability;

--identify elements of network performance which needed to be monitored; and

--identify automated and manual methods necessary for obtaining this information.

The WIN Implementation Plan, approved in January 1978, showed that WIN will be expanded in three phases. The first phase, which covered the period from April 1, 1978, through December 31, 1978, intended to implement an operational WIN and to expand the network to 17 sites considered necessary for time-sensitive command and control situations. Phase II, which covers the period from January 1, 1979, through June 30,

1980, intends to continue the expansion of WIN to four additional sites and to employ network capabilities to be provided by the next GCOS System Release. This phase is expected to continue until AUTODIN II becomes operational. WIN is scheduled to transition to AUTODIN II when it becomes available some time in 1980. Phase III will mark the transition from a dedicated support system to AUTODIN II.

According to information provided to us, the Department will spend approximately $40 million on the WIN effort from its inception in 1971 through its completion in 1982.

A NETWORK'S RELIABILITY IS NOT THE SAME AS ITS AVAILABILITY

Although the requirements for reliability are different for each application, the definition of the term "reliability" is the same. A generally accepted definition of reliability is:

> "The characteristic of an item expressed by the probability that it will perform a required function under stated conditions for a stated period of time." 1/

It will be noted that by definition, reliability is a probability of success.

It is essential to "build-in" reliability by sound design and construction and to carry out enough tests to make sure that this has been done.

A generally accepted definition of availability is:

> "The 'availability' or time an equipment is functioning correctly while in use depends both on reliability and on maintainability. Reliability * * * may be said to be a measure of an equipment's ability to perform its functions consistently under given conditions. Maintainability is a measure of the speed with which loss of performance is detected, diagnosed, and made good,* * *." 1/

1/Dummer, G.W.A., and Winton, R.C., An Elementary Guide to Reliability: Second Edition, Pergamon Press, 1974, p. 2.

As defined, availability is not reliability. This distinction becomes quite apparent when examining the methods the Department uses to determine PWIN's availability rather than its reliability and the Department's subsequent experience with WIN during the Guyana crisis and the NIFTY NUGGET exercise.

During the 1976 PWIN operational tests, the Joint Chiefs of Staff collected availability data on each major PWIN component--the host computer, IMP, and communication lines--and concluded that PWIN had an extremely high rate of availability. According to this data, the average availability of PWIN equipment ranged from 94.8 percent to 98.7 percent for the first test and from 92.1 percent to 99.3 percent for the second test. This data was somewhat misleading because the Joint Chiefs of Staff lacked the necessary techniques, methodology, and data bases necessary to properly collect and evaluate the effect PWIN's reliability had on the network's availability.

WIN was tested in the exercise NIFTY NUGGET 78. This exercise presented the Department with still another chance to realistically appraise the ability of WIN to support the functions of command and control in a major crisis situation. According to participants in NIFTY NUGGET, the response time of the system to commanders bordered on being unsatisfactory. The following observations were made by the U.S. Army Forces Command NIFTY NUGGET participants:

--The WWMCCS Entry System enabled the user to have any questions answered almost immediately. However, those secure communciations that used AUTODIN moved at the speed of hard copy or normal message traffic. The result of these factors was that the average age of data in WWMCCS was 8 to 12 hours old.

--WIN was inadequate because the WWMCCS standard computer system could not provide adequate ADP support for command and control during crisis.

--The WWMCCS standard computer system could not keep up with both daily maintenance and exercise requirements.

--The major factors causing the slow response time were (1) increased complexity of questions, (2) inadequate core (main memory) storage to service the users, (3) insufficient time to process data due to increased workloads, and (4) the lack of a single comprehensive data base.

--Several semi-independent application systems affected the WWMCCS ADP capabilities. Each of these systems had its own set of data files, which contained different data. As a result, problems were encountered with obtaining information in a timely fashion. To correct these differences, the U.S. Army Forces Command estimated it would have to increase its fiscal year 1979 program funding from $2.314 million to $5.934 million.

Perhaps the single, most favorable benefit identified by WIN users in this exercise was that it provided them a teleconferencing capability. Teleconferencing can simply be described as the ability to simultaneously transmit and receive information among a group of individuals who are geographically dispersed. Most users viewed this capability as enhancing the communication and problem solving method. However, even this benefit has limited capability in times of crisis. For example, we found that users perceived that WIN could not be used by individual commands as a full backup system for computer processing during a crisis. We were informed that if the Military Airlift Command lost its force control system, the U.S. Readiness Command would not have the excess computer capacity to process the increased data processing requirements.

Reliability is critical to the WIN project. Reliability problems for WIN have not been resolved. For example, during the Guyana crisis, problems occurred with the teleconferencing software. On one occurrence the Joint Chiefs of Staff crisis action team was out of contact with the Guyana teleconference team for over 1 hour. The problem occurred when a power outage caused access to the teleconference to be lost. When the crisis action team attempted to rejoin the conference, the computer could not be accessed because it did not accept the request to "sign on" from the terminal. A determination was made, subsequently, that when the outage occurred, the teleconference participant name for the crisis action team still remained "signed on" in the computer. However, the WWMCCS software did not permit a new "sign on" by the crisis action team, even though they had been physically disconnected from the computer.

To overcome these reliability problems, a new name for the crisis action team had to be entered so that access could be reestablished.

This condition occurred more than once and affected the Joint Chiefs of Staff crisis action team and the National Military Command Center ADP liaison officer participants. Selected teleconferencing commands caused similar

problems. For example, during one period the transfer from the teleconference to a time-sharing application caused problems with the teleconference computer program. The U.S. Readiness Command directed participants not to use the teleconference capabilities until the condition was corrected.

In another example, the ADP liaison officer in the National Military Command Center unsuccessfully attempted to use WIN to access the U.S. Readiness Command computer where the teleconference was hosted. The WIN message "Remote Host Dead" was given by the system, indicating that the U.S. Readiness Command computer was not operational. However, a telephone call to the U.S. Readiness Command indicated that its computer was fully operational. After 20 minutes of attempting to access the Readiness Command through WIN, the ADP liaison officer had his computer terminal switched to one of two available lines directly connected to the Readiness Command computer to circumvent the need to use WIN communications lines.

During the Guyana crisis, the Department of Defense reported average component availability for the network to be 95.5 percent even though it had experienced serious reliability problems.

A major factor contributing to the Department's inability to evaluate WIN's reliability is the lack of a means to collect the information needed to identify the specific components causing the failures.

On December 29, 1977, the Defense Communications Agency contracted with TRW for a network control study which would identify and develop a data base, techniques, and methodology for gathering this information. This study was completed in August 1978. It concluded that previously collected data was inadequate and insufficient to measure the network's reliability. The Joint Chiefs of Staff subsequently confirmed the fact that the Department still lacks a means to properly evaluate reliability. The study also provided the Department with suggestions as to how to gather the needed information. Our evaluation of the study showed that properly followed, the Department will be able to gather and analyze information which will confirm the fact that WIN is not reliable. We believe that confirming WIN's unreliability will not resolve design deficiencies inherent in WIN. The Department must replace the WWMCCS host computers and related software with items designed to function in an online interactive mode and redesign the network to simplify equipment configurations.

WIN DOES NOT PROVIDE NEEDED MULTILEVEL SECURITY CAPABILITIES

In a July 21, 1975, report to the Secretary of Defense (LCD-75-116), we noted that GCOS, the computer operating system software delivered with the WWMCCS computers, did not provide for, and could not be made to provide for, the secure multilevel type of operations required by the WWMCCS community.

We stated in our report that the WWMCCS computer system objectives for multilevel security and interactive operations were valid needs which should be satisfied. Since our concern was with the future direction of WWMCCS, we stated that these computer system objectives should be satisfied as soon as software technology permits and economical means can be found to use that technology.

The Director of Telecommunciations and Command and Control Systems agreed with our position and said the suggested alternatives would be evaluated, along with other information, to assure that the WWMCCS computer system plans provided for the most economical and viable solutions for the computer security problem.

In our April 5, 1978, report to the Secretary of Defense (LCD-78-106), we recommended that an office within the Office of the Secretary of Defense be given budget authority and responsibility for

- --controlling all computer security research and development in the Department;
- --reviewing and approving the computer security requirements for the Army, the Navy, and the Air Force;
- --reviewing and approving all computer security specifications, the methodology for determining the specifications, and requests for procurements for all WWMCCS computers; and
- --reviewing and approving all computer security long-range plans for WWMCCS and the three services.

On July 18, 1978, the Principal Deputy Under Secretary of Defense, Research and Engineering, responded to our April 5, 1978, report and informed us that in 1977 KSOS (or "Secure UNIX") was initiated. This effort will cost $2 million and 2 years to develop and is directly transferable to other machine architectures (it is not vendor-owned and requires no special hardware). Further, according

to the Principal Deputy, KSOS provides the Department with an excellent opportunity to quickly affect multilevel secure environments. The Department has large numbers of KSOS compatible hardware already in the inventory and many applications which will be able to immediately utilize the system in late 1979 (i.e., Secure Network Front-End and Message Handling Systems). The KSOS system will be employed in the WWMCCS Network Front-End to provide secure access to present WWMCCS systems in the early 1980s.

The Principal Deputy further informed us that the Office of the Secretary of Defense (Communications, Command, Control, and Intelligence) established a computer security initiative to (1) coordinate continuing Department of Defense computer security research activities, (2) serve as the technical focus for approval of secure systems within the Department, and (3) foster the computer manufacturers' development of secure computer systems using a methodology similar to KSOS.

However, a secure front-end to the WWMCCS standard computer system still does not solve the multilevel security problem.

Essentially, there is no comprehensive hardware and software solution at this time to the multilevel security problem in WIN.

The Department has conducted many studies on the issue of multilevel security. Two of these studies are discussed below.

The Center for Advanced Computation of the University of Illinois prepared a report in May 1975 which was based on interviews with military and civilian users of WWMCCS and on a review of six PWIN software systems and four software systems that are dependent upon the military version of GCOS. The purpose of this approach was to determine the needs of the WWMCCS community as perceived by the actual users of PWIN.

The report concluded that there was a definite need for multilevel security within the WWMCCS community. Investigators found that the military version of GCOS could not be made to provide secure operations for national applications. The report further concluded that the utilization of WWMCCS resources would be inefficient and the ability to share resources over a computer network would be minimal or nonexistent. For example, the report indicated that to change security classification whole machines and rooms must be sanitized. This means that lines may have to be broken,

disk packs have to be exchanged, and main memories have to be cleared. This process can easily take 1 or 2 hours. Not only does the sanitizing process remove valuable computational resources from productive work, but it also blocks ready sharing of secret and top secret data, such as operational and intelligence data.

These conclusions were further supported in a June 1978 study by the Institute for Defense Analyses. The objectives of this study were to provide a technical description of the Force Status System in an internetted environment. For example, two basic systems using Force Status in the planned WIN are discussed. The first is a Joint Chiefs of Staff or headquarters version of Force Status, which is classified at the top secret level. The second system is the U.S. Army Forces Command system, called the WWMCCS Entry System, which is classified at the secret level. Merger of these two systems, as currently configured, would require the U.S. Army Forces Command to upgrade its system, thereby requiring extensive new investments and upgrade in equipment, modifications in data handling procedures, and revisions in personnel clearance. The report concluded that these changes would be quite expensive.

The Strategic Air Command was scheduled to join WIN with a terminal in October 1978 and a host computer in 1980. However, Strategic Air Command officials recently stated that the command would not provide a host computer without the protection of multilevel computer security. Such protection is required for the sensitive Single Integrated Operations Plan data processed at the Strategic Air Command.

Major commands reporting to the U.S. European Command also require multilevel security. WIN users at the U.S. European Command will need file transfer/update and teleconferencing capabilities. Under current conditions, the Single Integrated Operations Plan is processed on the WWMCCS machine only 16 hours a week. During this time, no other WWMCCS processing, including WIN, is permissible because of security regulations. This condition will degrade the effectiveness of WIN operations of the U.S. European Command as a crisis communication system. To alleviate this problem, the U.S. European Command submitted a request for acquiring another WWMCCS standard computer system for processing the Single Integrated Operations Plan with the option to purchase an additional 128K memory and other equipment for an estimated purchase price of $1.1 million, plus $3,035 for monthly maintenance.

Similarly, the Defense Intelligence Agency requires multilevel security to interface with WIN. The Defense

Intelligence Agency has stated it will not use WIN because the system lacks multilevel security.

As currently structured, WIN cannot meet the multilevel security requirements of individual commands. This inability makes the use of WIN questionable in transferring certain data during time-sensitive situations. Current methods of transmitting data via the intercomputer networks will remain time consuming and expensive until multilevel security is developed and implemented. This requirement must be achieved for WIN to realize its full operational potential.

WIN is not sufficiently responsive, reliable, or secure, as demonstrated by its performance record. We believe that further extension of WIN will only compound the problems users have already experienced. The only viable long-range solution is to redesign and simplify the network, including the acquisition of new equipment and software designed to function in an online interactive mode as required in a command and control environment.

CHAPTER 7

WHAT ACTIONS WERE TAKEN TO CORRECT PROBLEMS IDENTIFIED IN PREVIOUS WWMCCS ADP PROGRAM STUDIES?

Most of the problems that we have discussed in this report are not new and have been previously reported to the Department along with recommendations for correction by us and various Department of Defense study groups. (See app. V for a representative list of reports previously issued regarding the WWMCCS ADP program.)

DEPARTMENT OF DEFENSE HAS TAKEN LIMITED ACTION ON PROBLEMS IDENTIFIED IN OUR REPORTS

We first started reporting on the issue of computer support for WWMCCS on December 29, 1970. We reported to the Chairman, House Committee on Appropriations, on a proposed computer system acquisition to support WWMCCS and the closely related Intelligence Data Handling System. Our review of the program for the acquisition of up to 87 computers concluded that it was not adequately planned or supported by valid cost and savings estimates or determinations of need. Further, we mentioned that the responsibility for planning and directing the acquisition program was fragmented among several of the Department's organizations, such as the Organization of the Joint Chiefs of Staff and the Directorate of Defense Research and Engineering. Today, the equivalent research and engineering office with WWMCCS oversight is the Principal Deputy Under Secretary of Defense for Research and Engineering (Communications, Command, Control, and Intelligence).

Following our 1970 report on WWMCCS, we reported on the program to Congressman Jack Brooks on May 6, 1971 (B-163074), the Secretary of Defense on July 21, 1975 (LCD-75-116) and on April 5, 1978 (LCD-78-106), and the Congress on September 21, 1978 (LCD-78-117).

Those subsequent reports addressed such issues as

--the lack of information requirements definition,

--fragmented planning and program management, and

--the inability of GCOS to provide the secure operating capability needed in the WWMCCS program.

Since many of the problems described in our earlier reports are still present today, it is apparent that the Department has not responded to the recommendations contained in those reports.

DEPARTMENT OF DEFENSE HAS TAKEN LIMITED ACTION ON PROBLEMS IDENTIFIED IN OTHER STUDIES

We have not been the only organization to report these and other substantive issues to the Department. Other organizations and individuals have studied and reported on command and control problems in general and WWMCCS in particular. The following examples indicate where other organizations have reported on the same issues that have been discussed in this report with no effective action taken by the Department.

Complex and fragmented management structure

The Defense Science Board Task Force on Command and Control Systems Management determined in its July 1978 report that

> "* * * our command and control systems have not kept up with the changes in the type of warfare or the changes in weapons and available command and control technology: * * * there is a strong need for a central organization which could essentially oversee the design and testing of all command and control systems that cut across service lines * * *."

Standard computer system and software are not responsive, reliable, or survivable

In 1976 IBM issued a series of reports on the WWMCCS architecture, as referred to earlier. These reports addressed all aspects of WWMCCS, including ADP. The architect study concluded that ADP was marginally effective in times of crisis because the program did not meet the needs of individual users. The study identified several deficiencies with the WWMCCS hardware, systems software, and application software. The study pointed out that

--ADP was not utilized, for the most part, to any great extent during actual crisis situations;

--data contained in the system was not sufficiently current, accurate, reliable, or complete;

--information was too voluminous and difficult to extract and assimilate during time-sensitive conditions;

--access to information required cumbersome procedures;

--users were not guaranteed availability when required;

--data contained in the Joint Reporting Structure was old, too detailed, poorly structured, and could not be integrated into common systems which provided meaningful displays for decisionmakers; and

--ADP application systems, such as WWMCCS, the Joint Operation Planning System, and the Force Status and Identity System were so large that, at a number of sites, only one of these systems could be loaded at a time.

In March 1976, the Rand Corporation prepared a report entitled "Report on WWMCCS ADP Communications Interface Requirements," and made the following observations:

"Almost every HIS [Honeywell Information System WWMCCS] 6000 installation we visited indicated severe limitations on the amount of main memory available, or on processing capacity. Additional communications processing such as a PWIN Network Control Program or additional special purpose device handlers for new terminals or network connections, put additional requirements on these already overcommitted resources.

"The GCOS operating system [the military version] was not designed for terminal handling, or for the exchange of message traffic with other computer systems. Rather, it was originally intended to be a batch processing system. Consequently, it has considerable difficulty dealing with the communications loads it is now expected to handle. In the current implementation of PWIN, with the Network Control Program as part of GCOS and resident in the HIS 6000, a higher interrupt rate and an associated increase in overhead is to be expected as a result of the addition of network processing requirements."

In a 1975 study performed for the Defense Communications Agency by the Center for Advanced Computation at the University of Illinois, the following observation was made:

"The ADP community in general and the WWMCCS ADP community in particular have a strong batch orientation. Many of the systems being developed for the WWMCCS Intercomputer Network take a batch approach. Unfortunately, the command function is a highly interactive function and bears little resemblance to batch operations. Also intercomputer networking is an inherently interactive technology as opposed to a batch technology."

In a report entitled "FORSTAT--Present Operation and Transition To The WWMCCS Intercomputer Network" written by the Institute for Defense Analyses, Science, and Technology Division in June 1978, two data retrieval systems available to users of U.S. Army Forces Command for WWMCCS Entry System were compared. The Institute made the following observations:

"The two retrieval systems available to the WES [WWMCCS Entry System] user are the SCN5 system (usually called SCAN) [the nonstandard system] and the Worldwide Data Management System (WWDMS) [the standard system]. The SCN5 system is the simpler of the two, requiring little or no programing skill. In practice, it is used 5-10 times as frequently as WWDMS * * *.

"The principal value of SCN5 over WWDMS is that it is a wholly on-line system. Runs are therefore processed much faster than with WWDMS (in an exemplary case with the same retrieval requirements, a few seconds compared to up to 20 minutes)* * *.

"* * * A second problem reported by users was the relative sophistication of the WWDMS Programming language compared to SCN5. Even though prototype programs are available through the system that can be modified by the user for his programming tasks, the system is still much more difficult for the inexperienced user to employ. The difficulty is compounded where multiple files must be accessed. Here, the level of programming skill required is particularly high; only a few experienced programmers at FORSCOM [the U.S. Army Forces Command] were said to have the skill to perform the necessary retrieval."

The Department continues to require WWMCCS users to buy and use WWDMS even though it is more difficult and inefficient to use than are other systems, such as the SCN5 system.

Standard computer system cannot provide multilevel security

The 1975 study by the University of Illinois, which was referred to earlier, made this statement regarding multilevel security:

> "Until an appropriate security technology is developed, the utilization of WWMCCS computing resources will be inefficient and the ability to share resources over a computer network will be minimal or nonexistent."

WIN is neither responsive nor reliable

In an August 1978 study performed for the Defense Communications Agency by TRW Defense and Space Systems Group on network reliability, the following observation was made:

> "Operational experience with the PWIN test bed has revealed a variety of network - reliability problems. Some of the causes of operational unreliability are egregious [i.e., remarkably bad, flagrant, outstanding for undesirable qualities]. Examples of such include gross hardware malfunctions in a host computer, front-end processor, IMP, modem, cryptographic device, or line, and certain software and procedural malfunctions * * * Many causes of operational unreliability, however, can be quite subtle. Examples include store-and-forward lockup in a message buffer, and a deadlock in a host-to-host protocol (each of two host computers is idle, waiting for the other to 'say something')."

In a report entitled "Concepts and Alternatives for a WWMCCS Communications Interface System" issued by the Rand Corporation in November 1977, the following comments were extracted regarding PWIN:

> "The current implementation of PWIN facilities involves specialized host-resident software at six WWMCCS sites that are connected to a dedicated communication subnet. Problems with this approach include low reliability and the high processing and core [main memory] loads imposed on the host equipment with ensuing limitations on responsiveness. In some cases (e.g., file transfer), the protocols have been specialized for H6000 equipment and would not generalize easily to other hosts. Terminal access to the network is through the H6000,

making access to remote systems for backup impossible when the local host has failed.

"* * * No terminal-terminal connectivity is provided forcing all data to be processed by or at least pass through the H6000. Security of the terminal handling system has never been verified."

Although the Department has been aware of major problems pertaining to WWMCCS ADP and related system support functions for 9 years, it has not effectively redirected the WWMCCS ADP program.

CHAPTER 8

ACCESS TO RECORDS: PROBLEMS ENCOUNTERED

Our longstanding position is that we cannot fully discharge our statutory responsibilities without access to the reports and supporting information that we consider to be necessary for the programs or activities being evaluated.

We were unable to fully discharge our statutory responsibilities and be totally responsive to the Chairman, Subcommittee on Research and Development, House Committee on Armed Services, and to Congressman Thomas J. Downey because the Joint Chiefs of Staff denied us complete access to documents we considered to be pertinent to this evaluation. These documents, which included internal surveys, reviews, draft reports, military exercises, operational plans, and future ADP plans, are materials to which we have a statutory right of access under section 313 of the Budget and Accounting Act, 1921 (31 U.S.C. 54). In our view, the Department's denial, without legal justification to provide us with complete access to the documents, had an adverse impact on our ability to complete our review of the WWMCCS ADP program in a timely and efficient manner.

As of June 1979 we were able to obtain complete access to only 66 percent of the total information we considered pertinent to the successful completion of our evaluation of the WWMCCS ADP program. In several instances, we withdrew selected requests because of the difficulty in obtaining the information. Failure to obtain access to pertinent information precluded our ability to properly determine whether future expenditures and the Department's planned future actions would resolve the problems described in this report.

As a result, we could not obtain source documents on important issues concerning the future of the WWMCCS ADP program. For example, during the week of November 13, 1978, and on December 20, 1978, we were denied access to the comments of the U.S. Navy, Europe, on a major command and control exercise--NIFTY NUGGET. According to the Director, Joint Chiefs of Staff, we were denied user comments because these comments did not represent the official position of the Department. Subsequent to this denial, the Secretary of Defense provided in testimony to the Congress the results of NIFTY NUGGET. Despite the Secretary of Defense's testimony, we are still unable to obtain any documents relative to the performance of WWMCCS during the NIFTY NUGGET exercise.

Users' comments on the ability of WWMCCS ADP to perform in a crisis are extremely important to our evaluation. The ability of an ADP system to satisfy users when necessary is critically important in examining the usefulness and reliability of that system, particularly during a time of crisis. Although users' comments may not represent the official position of the Department, their comments are critical in determining whether or not the system is adequately supporting their missions and needs.

In another instance, we requested access to operations plans, which include the critical elements of information for theater decisionmaking. For example, we requested U.S. Navy Europe Operations Plan 4102. We were denied access on December 20, 1978, by the Director of the Joint Staff who stated his decision was

> "* * * based on a long-standing JCS policy that knowledge of certain details of plans for the conduct of military operations should be limited to planners and those forces implementing the plan." (Emphasis added.)

We requested other documents, such as the Preliminary National Military Command System Master Plan and Technical Support Requirements for the Command and Control Technical Center. This preliminary master plan contained vital information on the system architecture and the Technical Support Requirements contained information on system software deficiencies and the costs of actions necessary to correct these deficiencies. Although these documents were made available for us to look at, we were not allowed to abstract or use the information in any way. The Director of the Joint Staff informed us that the Preliminary National Military Command System Master Plan had not been approved by the Joint Chiefs of Staff; hence, it was not an official document. Furthermore, the Director indicated that information from the plan could not be used in bibliographies, footnotes, or any other reference. It is interesting to note, however, that the IBM architect used this document as a source in developing the WWMCCS architecture in 1976. On February 2, 1979, the Director, Information Systems Division, denied us complete access to the Technical Support Requirements for the Command and Control Technical Center because they were considered internal working documents and could not be quoted or cited as references.

The Joint Chiefs of Staff refused us access to records primarily on the basis of their determination that the information we requested was outside the scope of our review.

For example, on December 12, 1978, we requested the evaluation of WWMCCS ADP and communications regarding the Guyana crisis in November 1978. All we received from the Joint Chiefs of Staff was the ADP section of the report. We also requested the same information regarding the seizure of the U.S. Mayaguez in 1975. We were denied complete access to this crisis report.

On January 5, 1979, when we requested access to key people in the Organization of the Joint Chiefs of Staff, we were advised that a letter requesting access had to be transmitted. The letter was to state the general purpose of our intended meeting, including the topics to be discussed. We were informed that access to selected key users relating to the Force Status and Identity System and the Joint Operation Planning System would be accorded only if we made our request in writing, which we did in our letter dated January 9, 1979. We were subsequently granted access to these individuals during the week of January 16, 1979.

On this assignment, the Joint Chiefs of Staff and the Command and Control Technical Center required us to place our requests in writing before they would respond. This resulted in unnecessary delays and inadequate responses by these agencies. For example, on October 6, 1978, we requested annual ADP plans for the National Military Command System. Approximately 36 days elapsed before we were provided partial information. Although a long delay was incurred, a Center official informed us that the plans were transmitted for release 21 days earlier than our receipt of these plans. The Command and Control Technical Center ADP procurement plan for fiscal years 1979 through 1984 was not provided until 44 days after our original request. However, the associated funding information was not released. According to a Department official, a decision was made to not release funding figures to us.

On February 8, 1979, the Chairman of the Subcommittee on Research and Development, House Committee on Armed Services, sent a letter to the Secretary of Defense concerning our access to records problem. Subsequently, we met with the Assistant Secretary of Defense (Comptroller) to resolve these problems. While the Chairman's letter has been of substantial assistance, many of our problems remain unresolved. We are still denied access to internal working papers, draft reports, operation plans and other critical documents. We still have not received the Operations Plan 4102, the Preliminary National Military Command System Master Plan, and critical information relating to North Atlantic Treaty Organization requirements. It is the position of the Department of Defense that this type of information will not be released to GAO.

We believe it is critical that we have access to all documents relating to our evaluation of the WWMCCS program. The Department has spent approximately $10 to $15 billion on the WWMCCS program since its inception. For the Congress to properly fulfill its oversight responsibility, it must be informed as to how economically, efficiently, and effectively this program is being managed. For us to properly serve the Congress, it is necessary that we obtain all information critical to evaluating this program. Our failure to gain this access means that we cannot adequately assist the Congress in its oversight responsibilities.

CHAPTER 9

WHAT CAN BE DONE TO IMPROVE THE WWMCCS ADP PROGRAM?

CONCLUSIONS

WWMCCS and its priority component, the National Military Command System, are essential elements of our national security. WWMCCS is intended to provide the National Command Authorities a means to receive warning and intelligence information and to provide direction to our military forces while supporting the Joint Chiefs of Staff in carrying out their responsibilities. Consequently, WWMCCS must be the most responsive, reliable, secure, and survivable system that can be made available within established resources. Data communications and ADP capabilities are two of the essential resources that can enable WWMCCS to achieve these objectives. To meet such requirements, the equipment must be compatible, communication links must provide a direct connection or real-time relay whenever necessary, computerized data formats must be common, and all components of the system configuration and operation must be as efficient as possible in terms of both effectiveness and in the utilization of resources.

Our evaluation of the WWMCCS ADP program showed that these objectives, recognized by the Department of Defense in 1966, are yet to be achieved although it has spent $1 billion for this purpose since the start of the program.

We believe the Department's future ADP expenditures, currently in excess of $140 million annually, will not resolve these problems unless the Department initiates major changes in the program's management structure and direction. We further believe that these problems can be resolved only if the military services work together more cooperatively.

In addition, the Congress should consider reducing the current and future years' WWMCCS funding to encourage the Department to make these needed changes in the program's management structure and direction.

RECOMMENDATIONS

With regard to the complex and fragmented WWMCCS management structure and needed changes in the program's direction, we recommend that the Secretary of Defense make certain that one central organization is given project management authority

and responsibility for all WWMCCS and WWMCCS related computer-based information systems. As the WWMCCS project manager, the designated central organization should be given the authority and responsibility for:

--Assisting in determining and consolidating the information requirements of the various commands which must use and rely on WWMCCS computer-based information systems to accomplish assigned missions, including the National Military Command System.

--Preparing comprehensive long- and short-range plans for the design, development, implementation, and operation of computer-based information systems that are responsive to and reliable for the WWMCCS primary and secondary missions.

--Implementing Department of Defense Directive 7920.1 on Life Cycle Management and other sound management practices as reflected in other such directives for all WWMCCS related computer-based information systems. This responsibility should include life cycle costing and the preparation of cost-benefit analyses for the Department and the Congress to be reasonably certain that (1) automated support for the command and control functions is provided within reasonable cost and budgetary limitations, (2) system development cycles are not unduly prolonged, and (3) the systems, when placed into operation, are the most responsive, reliable, and survivable ones that can be developed within resource limitations.

--Developing and implementing a system that provides a basis for tracking actual costs incurred for designing, developing, implementing, and operating computer-based information systems in support of the WWMCCS missions. Such a system should provide a means for comparing actual expenditures against budgeted costs and a basis for identifying and analyzing variances occurring between actual and budgeted program costs.

--Simplifying the exchange of information throughout the various commands. This responsibility includes developing a standard data base management system, standard programs, standard terminology, and standard data formats. In addition, this responsibility includes identifying and acquiring the computer and related data communications equipment needed to properly support those commands. This includes replacing any or all of the existing computer and related

data communications equipment, as necessary, to provide the online interactive information processing capability required by those commands. Any equipment acquisitions or replacements should not be initiated until after the information requirements and the time frames within which the information to be processed have been identified, agreed upon, and incorporated into the comprehensive long- and short-range plans for the development, implementation, and operation of computer-based information systems for support of the WWMCCS missions.

In addition, the Department should designate a single organization to centrally manage the research and development efforts associated with computer security within the Department. This responsibility, among other things, should include the review and approval of all computer security requirements within the Department of Defense, including the three military services, all computer security specifications, the methodology for determining the specifications, requests for all research and development efforts associated with computer security, and all computer security long-range plans for the Department and the three services. In addition, this responsibility should include any necessary and related budgetary authority.

To encourage the Department to make the needed changes in the WWMCCS ADP program management structure and direction, we recommend the Congress consider reducing the current and future years' WWMCCS funding in the following manner:

--Withhold funds for completion of the study to determine the operational utility of ADP in support of WWMCCS. There is no need for this study. The WWMCCS architecture study completed in 1976 and related follow-on studies completed since 1976 already provide this information to the Department. These studies cost $23 million.

--Withhold funds for WIN until the Department completes its determination of the information needed by the various commands to support their command and control functions. This determination should result in a set of functional specifications that can be used competitively for the acquisition of computer and data communication systems that will more appropriately function in a command and control environment.

--Withhold funds intended to upgrade the current WWMCCS standard computer system until the Department identifies the configuration that will replace it.

LIST OF OUR PREVIOUS REPORTS ON WWMCCS COMMUNICATION CAPABILITIES AND RELATED ISSUES

Title	Report No.	Date
Investigation of Advanced Airborne Command Post	B-178570	9/25/73
Need To Consolidate Responsibility for Automatic Digital Network (AUTODIN) Terminals	B-169857	7/17/74
Defense Communciations Agency (DCA) Automatic Voice Network (AUTOVON) Switch Elimination Activities	LCD-75-109	1/16/75
Letter report to Chairman, House Committee on Armed Services-- GAO Comments Regarding Possible NATO Purchase of the AWACS	B-163058	4/25/75
Better Management of Defense Communications Would Reduce Costs	LCD-77-106	12/14/77
Secure Voice Telephone Systems-- How Department of Defense Can Save Millions	LCD-77-105	12/30/77
Update on Review of the Development of Military and Civil Agency Non-Tactical Secure Voice Systems	LCD-78-129-I & II	9/29/78
Potential Improvements in Design of Automatic Secure Voice Communications II and Tri-Service Tactical Communications Programs	LCD-79-107	2/23/79
An Assessment of the Joint Tactical Information Distribution System	PSAD-79-39	2/28/79
The Defense Satellite Communications System (DSCS III)	LCD-79-103	3/12/79

APPENDIX II

U.S. House of Representatives
COMMITTEE ON ARMED SERVICES
Washington, D.C. 20515
NINETY-FIFTH CONGRESS
MELVIN PRICE, CHAIRMAN

September 15, 1978

Honorable Elmer B. Staats
Comptroller General of the United States
General Accounting Office
441 G Street, N. W.
Washington, D. C. 20548

Dear Mr. Staats:

It has come to my attention that the General Accounting Office has been conducting a rather comprehensive review of the Department of Defense Worldwide Military Command and Control System (WWMCCS). In view of the deficiencies and problems with the WWMCCS that have been highlighted in the reports emanating from your office as well as other information provided to this committee, I expect that the Research and Development Subcommittee will initiate an in-depth review of this system as part of our review of the fiscal year 1980 Department of Defense budget request.

I would appreciate it, therefore, if prior to the end of this calendar year your staff could focus on those issues which I believe will be of primary concern to the subcommittee. I am most interested in the GAO assessment of the ability of the WWMCCS system to satisfy our military command and control requirements during a time of crisis, including such factors as: meantime to repair, meantime between failure, projected and actual system availability, and the effectiveness of physical system security. Additionally, I would appreciate your staff's assessment of the existing software package together with software deficiencies and the potential for near- and long-term modifications to eliminate or lessen existing problems.

APPENDIX II

In light of the subcommittee's schedule regarding the fiscal year 1980 Department of Defense budget request, I am hopeful that your staff could provide me with an oral report by January 15, 1979 and a final report without agency comment by June 30, 1979.

My points of contact for the committee staff are Mr. A. R. Battista and Dr. Thomas Cooper, who can be reached at 225-3168. Please accept my sincere appreciation for your continued assistance.

Sincerely,

Richard H. Ichord
Chairman, Subcommittee on
Research and Development

RHI:abo

APPENDIX III

THOMAS J. DOWNEY
2ND DISTRICT, NEW YORK

326 CANNON HOUSE OFFICE BUILDING
TELEPHONE: (202) 225-3335

DISTRICT OFFICE:
4 UDALL ROAD
WEST ISLIP, NEW YORK 11795
TELEPHONE: (516) 661-8777

Congress of the United States
House of Representatives
Washington, D.C. 20515

COMMITTEE ON
ARMED SERVICES
SUBCOMMITTEES:
MILITARY PERSONNEL
MILITARY COMPENSATION

SELECT COMMITTEE ON AGING

COMMITTEE ON
SCIENCE AND TECHNOLOGY
SUBCOMMITTEES:
FOSSIL AND NUCLEAR ENERGY
SPACE SCIENCE AND APPLICATION

August 9, 1978

The Honorable Elmer B. Staats
Comptroller General of the United States
Washington, DC 20548

Dear Mr. Staats:

The World Wide Military Command and Control System (WWMCCS) is a composite of military command facilities, communications, warning systems, and computers located throughout the world to support military command and control activities. It is an important and integral part of our Nation's military readiness capability.

During your recent review of the multi-level computer security requirements of WWMCCS (LCD-78-106, April 5, 1978), you stated that several problems have been identified concerning the satisfaction of WWMCCS computer security requirements. Further, you state that the full operational capability and goals of the WWMCCS computers, in a time-sensitive network, will not be achieved without some form of multi-level security to protect the integrity of the DOD security classifications on data being processed.

The aftermath of the WWMCCS computer update program of 1970 also has raised serious questions about the ability of many WWMCCS computers to adequately perform their functions. As your December 29, 1970 report points out, the buy of Honeywell computers was ill planned and, in many instances, was penny wise and pound foolish.

The results of the computer update program have pointed out severe problems with the overall management of WWMCCS. For example, I am concerned that the decision to standardize the WWMCCS computer system with the Honeywell equipment purchased in 1970 may have an adverse impact on our national security. It has been brought to my attention that NORAD's missile-tracking accuracy may be diminished with the switch to these machines.

I am concerned with the impact of multi-level security and these related problems on the success of the WWMCCS computer systems in satisfying current and future user requirements. There appear to be several fundamental problems that have been experienced in the management of the WWMCCS computer and data communication systems investment.

Page one

In order to recommend a future course of action that would assist in resolving present problems and in avoiding problems experienced in similar computer and data communication system programs, would you please review the following issues:

1. The adequacy of the Department of Defense management structure for the control and operation of the WWMCCS computer and data communication systems.

2. The effectiveness of the process by which the WWMCCS decision-making system is analyzed to determine how the computer operations can best provide a timely and accurate decision support system.

3. The responsiveness of the long-range and short-range computer and data communication systems planning process in WWMCCS.

4. The utility of Department of Defense actions and plans in response to your recommendation that an office within the Office of the Secretary of Defense be given budget authority and responsibility for:

--Control of all computer security research and development in DOD.

--Review and approval of the computer security requirements for the Army, the Navy, and the Air Force.

--Review and approval of all computer security specifications, the methodology for determining the specifications, and requests for procurements for all WWMCCS computers.

--Review and approval of all computer security long-range plans for WWMCCS and the three services.

5. The degree of life cycle management control being exercised by the Department of Defense with respect to the WWMCCS computer and data communication systems.

6. The possibility that present attempts to standardize automatic data processing systems among all WWMCCS components, irrespective of their disparate needs, may give rise to serious problems in WWMCCS operations, especially the NORAD missile tracking system.

APPENDIX III

The Honorable Elmer B. Staats
August 9, 1978
Page three

I also request that you provide an update to your December 29, 1970 report on "Problems in the Acquisition of Standard Computers for WWMCCS." I would like an analysis of all the current ramifications of this 1970 computer buy and would like to know if and how WWMCCS procurement policies and procedures have improved since that time. Any current deficiencies in this area should be pointed out.

As your work progresses on these issues, I would appreciate periodic oral briefings. Your conclusions and recommendations should be developed and incorporated in a report to me as soon as possible. I respectfully request that you complete the report no later than August 31, 1979.

Thank you for your assistance in this matter.

Sincerely,

THOMAS J. DOWNEY
Member of Congress

TJD/rd:nh

APPENDIX IV

CHRONOLOGY OF EVENTS RELATING TO THE PROTOTYPE WORLD WIDE MILITARY COMMAND AND CONTROL SYSTEM INTERCOMPUTER NETWORK (PWIN) AND THE APPROVAL OF THE WWMCCS INTERCOMPUTER NETWORK (WIN) PROGRAM: 1971-1977

April 30, 1979

September 7, 1971:

JCSM-593-71, "Research, Development, Test and Evaluation Program in Support of the Worldwide Military Command and Control Standard System" establishes the need for developing the Prototype WWMCCS Intercomputer Network (PWIN). This authorization is based on a need for faster and more accurate information to support crisis management actions and continuity of operations for the National Command Authorities.

Specific requirements included online or remote responses in a timely manner from computer terminals and multilevel computer security features. Multilevel computer security enables users of the system, with different levels of access to classified information, to simultaneously share the same computer equipment (timesharing) and be denied access to information for which they are not authorized.

December 2, 1971:

DOD Directive 5100.30 establishes requirements for the National Military Command System of WWMCCS to be "the most responsive, reliable, and survivable system that can be provided within the resources available." (Emphasis added.)

September 4, 1973:

Defense Communciations Agency management is alerted by the PWIN Test Director to the possibility of failure of the PWIN computer network.

September 25, 1973:

The WWMCCS Objectives Plan for fiscal years 1974-1993 indicates that the WWMCCS Intercomputer Network (WIN) is an operational requirement.

October 11, 1973:

The Deputy Director of the Office of Engineering and Implementation, Defense Communications Agency wrote that, in 1975, PWIN would be transitioned into an operational system.

October 29, 1973:

The First comprehensive PWIN Test Plan is prepared and approved by the PWIN Test Director and the PWIN Project Manager. This plan emphasizes that reliability is a major problem area.

November 19, 1973:

A preliminary briefing on the PWIN project is presented to Defense Communications Agency management. This briefing was supposed to be given to the WWMCCS ADP (Automated Data Processing) Project Manager in the Joint Chiefs of Staff. Reliability is emphasized as a potential problem area.

November 28, 1973:

Approximately one week after Defense Communications Agency management had denied PWIN was to become operational, top management personnel is informed that the object of PWIN is to develop an operational WWMCCS network capability.

April 19, 1974:

The MITRE Corporation prepares a report that confirms the existence of major reliability problems in PWIN.

May 5, 1974:

A memorandum for the Chief, Software Support Division, Command and Control Technical Center, Defense Communications Agency, indicates that PWIN is not intended to become an operational network. However, this statement contradicts the WWMCCS Objectives Plan for fiscal years 1974-1993.

September 4, 1974:

The Joint Chiefs of Staff recommends to the Secretary of Defense that PWIN be expanded from three to six sites in order to provide more meaningful experiments and testing of the computer network.

September 18, 1974:

Defense Communications Agency management is urged to adopt a "Concept of Failure Plan" to provide advance planning for reliability problems rather than last minute panic reaction to network failure. Apparently, no action was taken by management to prepare such a plan.

October 9, 1974:

A memorandum describing the threat of electrical disturbances in computer power supply and providing solutions is developed by the Defense Communciations Agency staff. No action was taken because management felt that "it was not good politics."

December 4, 1974:

The Deputy Secretary of Defense approves the expansion of the PWIN project. However, this memorandum noted that detailed requirements were not well defined. Therefore, a PWIN development plan was required and prepared by the Defense Communications Agency.

January 20, 1975:

An engineering report is prepared describing the results of the First System Integration Test of the PWIN computer network. Major reliability problems are noted and the failure rate is estimated to be 50 percent. The report concludes that only a direct recognition of the problem and formal effort to develop solutions should resolve the reliability problems. Apparently no action was taken on this report by the Defense Communications Agency.

May 19, 1975:

The University of Illinois issues a report critical of PWIN's ability to operate in a responsive online manner. The report concludes this capability is necessary for command and control. The report briefly describes existing technology which is available to provide the online capability to meet command and control requirements.

July 21, 1975:

The General Accounting Office sends a letter report (LCD-75-116) to the Secretary of Defense strongly questioning whether PWIN will be able to meet its design objectives and criticizing PWIN's excessive response times.

September 25, 1975:

The Director, Telecommunications and Command and Control Systems, agrees with GAO that internetting, fully interactive operations, and multilevel computer security are goals which must be achieved. Further, in light of GAO's report, final approval of the PWIN development plan is delayed.

NOTE: This office has been replaced by the Office of the Assistant Secretary of Defense (Communications, Command and Control, and Intelligence).

October 20, 1975:

A memorandum to the Chairman, Joint Chiefs of Staff, severely criticizes the PWIN development plan drafted by the Defense Communications Agency in response to the Deputy Secretary of Defense's December 4, 1974, memorandum. This memorandum suggests that each WWMCCS ADP site be surveyed to identify its internetting requirements. We found no evidence which indicates this was ever accomplished by the Joint Chiefs of Staff.

March 29, 1976:

A memorandum from the Release Coordinator reports major reliability problems with the PWIN network. According to this memorandum, the network fails approximately every 35 minutes.

April 20, 1976:

GAO notified the Secretary of Defense that the Air Force is, for all practical purposes, terminating its multilevel computer security program because of insufficient fiscal year 1976 funds. Multilevel computer security is an important requirement for both PWIN and WIN.

June 10, 1976:

The Director, Telecommunications and Command and Control Systems, states that the Air Force was not terminating the multilevel computer security program and has entered a reclama to Congress to ask for a restoral of all fiscal year 1977 monies for this program.

July 6, 1976:

The Director of PWIN Operational Experiments states that "during recent practice sessions to prepare for a June 24, 1976, demonstration of the system, the reliability of system hardware and software was extremely poor. During approximately two weeks of demonstration practices, we were unable to complete one full run of the planned demonstration due to a variety of system hardware and software problems."

The Director then gave the PWIN project the following ultimatum. . . "To gain assurance that the operational experiments will be conducted under conditions that will provide a reasonable degree of confidence that experiment

objectives will be achieved, I have requested CCTC (Command and Control Technical Center) to demonstrate PWIN system reliability on 12 and 13 July. Based on this demonstration, a determination will be made relative to conduction of the formal PWIN Operational Experiments scheduled between 19-30 July 1976."

July 15, 1976:

This ultimatum failed to produce the desired results. A telegram is sent by the Joint Chiefs of Staff to all WWMCCS sites participating in the PWIN project. This telegram delayed the beginning of the operational experiments because of the following problems:

--Instability of communication links between PWIN nodes.

--Uncoordinated communication fault corrections.

--Intermessage processor and host or main hardware/software failures. These failures were due to loss of power, air conditioning, and component failures.

August 23, 1976:

The Air Force Systems Command instructs the Electronic Systems Division to take action to terminate their multilevel computer security program during fiscal year 1977, as the Command did not have adequate funds to continue efforts in this area. This occurred despite DOD's assurance to GAO on June 10, 1976.

NOTE: We interpret the termination of the Air Force multilevel computer security program as detrimental to successful computer internetting in a multilevel secure environment.

A computer security consortium chaired by the Office of the Assistant Secretary of Defense (Communications, Command, Control and Intelligence) reformed one of the Air Force contractor teams at the MITRE Corporation in fiscal year 1979.

August 31, 1976:

The Chief of the Software Support Division of the Command and Control Technical Center, the Defense Communications Agency, reports that the proliferation of

emergency patches to resolve General Comprehensive Operating Supervisor (GCOS)/PWIN interface problems to enhance performance is rapidly becoming a cause of great concern.

September and October 1976:

PWIN Operational Experiments 1 and 2 are conducted. During these evaluations reliability is identified as a critical problem by several commands.

January-February 1977:

Top management in the Department of Defense is briefed on the PWIN project. The briefing also identifies problems areas of system reliability, bulk data file transfer, and operating procedures. Despite these problems, it is recommended to proceed with an operational network.

February 18, 1977:

The Subcommittee on Investigations, House Committee on Armed Services (HASC No. 94-72) recommends that additional management attention should be directed toward the Department of Defense's automated data processing program. Particular attention must be directed to improving software security and the development of techniques which will allow effective computer internetting.

March 1-16, 1977:

The PRIME TARGET exercise is conducted and includes the six participating PWIN sites. This exercise shows that four of the six sites experienced high percentages of abnormal terminations averaging 62 percent. An abnormal termination can be defined as a termination of operations due to software or hardware or combination of software/ hardware failures.

NOTE: These severe reliability problems are apparently typical of prior exercises such as ELEGANT EAGLE 76.

Although the individual hardware/software components in the PWIN/WIN may be highly reliable, we consider failure to provide the user with the capability to successfully achieve a given task to be indicative of a larger system reliability problem. For example, the law of reliability shows that in serial systems, the reliability of the system is determined by multiplying the component failure rates together--not by adding them. If there are

seven components in a typical PWIN/WIN serial system or site with individual reliability of 0.99 then the overall site reliability equals (0.99) exponent 7 or 0.932065. In the six site test of PRIME TARGET 77, the serial system reliability for PWIN would be approximately (0.99) exponent 42 (42=7 components x 6 sites) or 0.655659. These reliability computations are not necessarily the actual network reliability measures. However, they serve to demonstrate the relationship of PWIN availability with its reliability.

June 1, 1977:

The Final Consolidated Report for PWIN Operational Experiments 1 and 2 is issued by the Joint Chiefs of Staff. While the report is generally favorable, it indicates problems with reliability, data file transfer, and multilevel computer security procedures. For example, PWIN was unable to successfully transfer Force Status and Identity Report System (FORSTAT) data from either the Master File or the STRIP file. According to Joint Chiefs of Staff criteria, PWIN must be able to successfully transfer FORSTAT information.

July 18, 1977:

Despite the existence of these problems, the Joint Chiefs of Staff approves and validates an operational requirement for a WWMCCS Intercomputer Network (WIN). According to several Department of Defense officials, the decision to go operational was advisable because the users of PWIN saw it was a tool to improve their decision making capability. These officials informed us that the problems identified in PWIN can only be solved by letting the system "evolve."

December 27, 1977:

Approximately five months after the Joint Chiefs of Staff validated the operational requirement for WIN, the Defense Communications Agency identified the following reliability and availability deficiencies with the PWIN program:

--Software releases and emergency changes (patches) did not always receive standard system software test and evaluation. At times, this practice resulted in release to the field of software that had not been adequately tested and contained errors. The result was repeated system failure.

--The present PWIN communication subnet topology was based on least cost as opposed to reliability. As a result, each site or group of sites tended to be isolated from some or all of the network.

--Electrical power problems have caused network outages. Aside from total system failure at user sites when power systems failed, the network has experienced Interface Message Processor (IMP) failure during electrical storms or other times when the power system was subjected to voltage and frequency fluctuations.

--Interface Message Processor (IMP) maintenance and operation has been inadequate. Contractor field engineers at certain sites were unable to repair the Interface Message Processor (IMP) because of inadequate training. On several occasions, personnel had to be sent to sites during exercises to repair the Interface Message Processor (IMP). Because site operators were not qualified to diagnose problems and in some instances, unable to load the software, excessive downtime resulted.

--Adequate quantities and types of spare parts are not available for the Interface Message Process (IMP). Consequently, sites have experienced excessive downtime due to lack of spares; also, spare parts have on occasion been found to be ineffective.

--Difficulty in determining the causes of Interface Message Processor (IMP) failures resulted in excessive downtime.

--The present network configuration does not allow for alternate site access. When an Interface Message Processor (IMP) or host fails, that site is isolated from the network. This is of prime concern especially when that site is a major player in a crisis situation.

--PWIN host software contains "errors" which cause the user to have difficulty in effectively using certain internetting features such as

teleconferencing. These errors cause programs to be aborted, resulting in excessive rerun times after aborts or loss of data.

--Interface Message Processor (IMP) and IMP/H6000 interface software contains known errors. The various software and hardware configurations in use provide a myriad of potential interface problems.

--Communication problems have adversely affected the reliability/availability of PWIN. Some of the major problems are: several communication lines repeatedly failed during Joint Chiefs of Staff exercises; not all sites have technical control facilities to monitor communications and help in restoration; and Interface Message Processors (IMPs) are located in Automated Data Processing areas where they are not monitored on a continued basis.

As a result of these problems, the Director, Defense Communications Agency conducted a WWMCCS Intercomputer Reliability Study to resolve these problems. We requested a copy of this study but were denied access because it was in "draft." Therefore, we are unable to ascertain whether these problems have been satisfactorily resolved.

- - - -

Many of these problems continue to exist in the WIN project. However, DOD made a decision to proceed with a system which did not meet its intended purpose. Essentially, the purpose is to develop a highly reliable intercomputer network that operates in an online interactive mode and provides multilevel security. Factors that caused the PWIN not to achieve its intended objectives include the Department of Defense decision to make PWIN operational soon after experiencing the reliability problems in PRIME TARGET 1977.

LIST OF GAO AND VARIOUS DEPARTMENT OF DEFENSE STUDY GROUP REPORTS ON THE WWMCCS ADP PROGRAM

Our Reports

"Problems in the Acquisition of Standard Computers for the World Wide Military Command and Control System." Report to the House Committee on Appropriations (B-163074, Dec. 29, 1970).

Letter report on the World Wide Military Command and Control System to the Chairman, Subcommittee on Government Activities, House Committee on Government Operations (B-163074, May 6, 1971).

Letter report on the World Wide Military Command and Control System to the Secretary of Defense (LCD-75-116, July 21, 1975).

Letter report on the World Wide Military Command and Control System to the Secretary of Defense (LCD-78-106, Apr. 5, 1978).

"NORAD's Information Processing Improvement Program--Will It Enhance Mission Capability?" Report to the Congress (LCD-78-117, Sept. 21, 1978).

Department of Defense Reports

"Report to the President and the Secretary of Defense on the Department of Defense By the Blue Ribbon Defense Panel" (July 1, 1970).

"Research in Network Data Management and Resource Sharing; Application Summary." Center for Advanced Computation, University of Illinois at Urbana-Champaign (May 19, 1975).

"Report on WWMCCS ADP Communications Interface Requirements." Rand Corporation (Mar. 1976).

"WWMCCS Software Maintenance and Enhancement Study." The MITRE Corporation (June 1976).

"Research in Network Data Management and Resource Sharing; Final Research Report." Center for Advanced Computation, University of Illinois at Urbana-Champaign (Sept. 30, 1976).

"Prototype WWMCCS Intercomputer Network (PWIN) Operational Experiments Program; Final Consolidated Report for Operational Experiments #1 and #2." Joint Chiefs of Staff (June 1, 1977).

"The Impact of the WWMCCS Architecture Study on WWMCCS ADP Operations." Rand Corporation (June 1977).

"Summary of Findings for WWDMS T-2 Performance Testing Phase 2." PRC Data Services Company (Aug. 29, 1977).

"FMIS Evaluation Phase 3 Report." PRC Data Services Company (Sept. 30, 1977).

"Preliminary Examination of WWMCCS Autodin I Traffic." Rand Corporation (Sept. 1977).

"WWMCCS Operational Data Management: Requirements Baseline and Problem Areas." Rand Corporation (Nov. 1977).

"Concepts and Alternatives for a WWMCCS Communications Interface System." Rand Corporation (Nov. 1977).

"FORSTAT--Present Operation and Transition to the WWMCCS Intercomputer Network." Institute for Defense Analyses; Science and Technology Division (June 1978).

"Report to the Secretary of Defense on the National Military Command Structure." Department of Defense - Richard C. Steadman (July 1978).

"Report of the Defense Science Board Task Force On Command and Control Systems Management" (July 1978).

"Network Reliability," TRW; Defense and Space Systems Group (Aug. 31, 1978).

"Transition Strategies for an Intermediate WWMCCS Communications Interface Subsystem." Rand Corporation (Nov. 1978).

"Summary Report of Audit; Force Status Report (FORSTAT) and Unit Capability Measurement System (UCMS)." Air Force Audit Agency (June 20, 1979).

APPENDIX VI

MEMORANDUM OF AGREEMENT BETWEEN THE ORGANIZATION OF THE JOINT CHIEFS OF STAFF AND THE DEFENSE COMMUNICATIONS AGENCY

1. In conjunction with the establishment of the new Joint Command, Control and Communications (C^3) Directorate in the Joint Staff a realignment of technical management functions and processes is to be made. This realignment is being implemented in an effort to improve the WWMCCS ADP Management structure by emphasizing the policy and requirements responsibilities of the Joint Chiefs of Staff and the technical responsibilities of the Defense Communications Agency (CCTC). This has the effect of disestablishing the WWMCCS Project Managers Office (PMO) as it currently exists. This realignment includes functional activities previously covered by the J-3 WWMCCS ADP Management Division and the J-3 Information Systems Division.

2. The C^2 ADP Division of the Joint C^3 Directorate will perform the functions listed in Enclosure 1.

3. The functions listed in Enclosure 2, previously accomplished by the J-3 WWMCCS ADP Management Division will be transferred to DCA (CCTC).

4. The functions listed in Enclosure 3, previously accomplished by the J-3 Information Systems Division will be transferred to DCA (CCTC).

5. This agreement will be consummated by a functional transfer of responsibilities and associated personnel from the OJCS (C^3) to DCA (CCTC). The actual transfer of function will occur when the personnel associated with the function are transferred.

6. In addition to these functional transfers, a change in the management process between the Joint C^3 C^2 ADP Division and DCA (CCTC) will be needed. An overview of this revised management process is contained in Enclosure 4.

7. Enclosure 5 lists the personnel billets which will be transferred to DCA to accomplish the increased responsibilities and the administrative actions required in conjunction with these transfers. Modifications to this list will be agreed to by both parties of the agreement.

8. Six months after implementation of this MOA, the principals to this agreement will review the alignment of functions and personnel and reach agreement on any necessary adjustments.

VAN DOUBLEDAY
Major General, USAF
Deputy Director, Operations,
Command, Control & Communications
OJCS

DONALD J. BOWEN
Brigadier General, USAF
Deputy Director
Command and Control
DCA

5 Enclosures
a/s

1 June 1979

APPENDIX VI

FUNCTIONS TO BE ACCOMPLISHED BY THE C2 ADP DIVISION, JOINT C3 DIRECTORATE

A. Functions Previously Assigned

1. Provide policy and guidance for controlling compromising emanations (TEMPEST) within the WWMCCS ADP System.

2. Provide policy and guidance for interfacing intelligence systems to the WWMCCS ADP system. Serve as liaison to the appropriate intelligence organizations dealing with operations/intelligence ADP matters.

3. Coordinate the development and validation of communications requirements to support the WWMCCS ADP system with the DCS Division of the Joint C3.

4. Develop and maintain WWMCCS ADP operational concepts, plans, policies, and doctrine to meet the ADP support requirements of the WWMCCS.

5. Provide WWMCCS ADP inputs, as required, to the JSPS and JOPS documents, and the WWMCCS Objectives and Management Plans.

6. Review plans of the Services, unified and specified commands, and other DoD agencies relating to WWMCCS ADP to assure development and requirements are within current policy and guidance.

7. Accomplish Joint C3 action and coordination with respect to the Data Elements and Data Codes Standardization Program, including the preparation of appropriate staff studies, analysis and evaluation of WWMCCS overall system performance based on current standards, and development of future standards and for the integration of WWMCCS reporting system requirements.

8. Act as Chairman of the WWMCCS ADP System Managers Group.

9. Provide representation to the WWMCCS ADP Systems Software, Applications Software, Data Base Management, Security and Terminal/Communications Technical Committees.

10. Monitor and review the planning, programming, and budgeting actions of the Services, unified and specified commands, and agencies in connection with the WWMCCS ADP Program. Coordinate with appropriate offices in OSD to insure the accomplishment of the WWMCCS ADP requirements and objectives. Monitor and review the costs of WWMCCS ADP development and standardization actions in connection with related PPBS documentation.

11. Provide liaison between the WWMCCS ADP community and the Defense Communications Agency (DCA) on matters involving programs, budgets and general management of resources.

12. Provide policy, procedural guidance, operational guidance, consolidated requirements, and tasking priorities to the Defense Communications Agency (DCTC).

B. Functions Modified/Revised Through Realignment

1. Provide policy guidance and program objective for the development of procedures and technical capabilities to improve the ADP Security posture of the WWMCCS ADP Standard system.

2. Provide policy and guidance for the WWMCCS Standard ADP Terminal Program.

3. Validate System Development Notifications (SDNs), System Change Proposals (SCPs), and Justification Approval and Acquisition Documents (JAADs).

4. Validate new equipment requirements for the WWMCCS Standard ADP system in accordance with the JCS Pub 17 SDN and SCP procedures.

5. Coordinate with Services/Agencies the development and maintenance of management procedures for the WWMCCS Standard system.

6. Validate requirements, review and forward plans and proposed modifications for the WWMCCS Standard system contract to the Successor Contracting Office.

7. Provide guidance regarding WWMCCS ADP logistic support. Review and forward logistics requirements and plans to the Single Service Manager.

8. Provide guidance regarding WWMCCS ADP training support. Review and forward training requirements and plans to the Single Service Manager.

9. Provide representation to the WWMCCS ADP Training and Logsitic Support Panels.

10. Provide representation for the Joint Chiefs of Staff on Service/agency-conducted on-site management surveys of WWMCCS ADP installations.

11. Review and validate the following ADP requirements for individual WWMCCS ADP installations:

a. Standard ADP equipment for procurement through the basic WWMCCS ADP contract(s).

b. Non-standard ADP equipment for site-unique C^2 functions.

c. Standard WWMCCS systems/applications software.

d. Unique software development when standard WWMCCS software cannot meet site requirements.

e. All WWMCCS ADP systems configuration changes, additions and deletions.

APPENDIX VI

12. Reviews and validates, through the Joint Process when necessary, new requirements for standardized ADP capabilities, including hardware acquisition and software development.

13. Assesses WWMCCS ADP operational performance against standards and initiates actions to correct deficiencies.

14. Provides policy and guidance in the execution of ADP security requirements and procedures.

15. Provides guidance for WWMCCS ADP application, systems hardware/software, and supporting communications systems planning.

16. Establishes policies and procedures to ensure that all C^2 ADP requirements are developed, validated, prioritized and supported.

17. Develops, coordinates and publishes C^2 ADP functional objectives and performance criteria.

APPENDIX VI

FUNCTIONS TRANSFERRED TO DCA (CCTC)

A. Complete Functional Transfer

1. Develop and maintain plans for the evolutionary development of the WWMCCS ADP system.

2. Manage the WWMCCS standard applications software program.

3. Manage the WWMCCS standard system software program and the associated software incident management system.

4. Develop, recommend approval, and promulgate documentation standards for the WWMCCS Standard ADP system.

5. Direct, coordinate, and promote the development and application of data management capabilities, including the standard Worldwide Data Management System (WWDMS), and associated contract activities.

6. Provide guidance and point of contact for data base administration throughout the WWMCCS ADP system.

B. Functions Modified/Transferred Through Realignment

1. Develop and implement programs to enhance the technical or procedural ADP security features of the WWMCCS ADP Standard systems.

2. Manage the development and implementation of the WWMCCS Standard ADP terminal program, including the coordination and reconciliation of user requirements.

3. Process, evaluate and recommend approvals/diapprovals on SDNs, SCPs, and JAADs. This includes relating and consolidating similar proposals, evaluating each proposal and assessing its impact on the WWMCCS community and implementing approved changes.

4. Perform technical analyses for new equipment requirements.

5. Develop and recommend changes to WWMCCS Standard system management procedures as needed.

6. Solicit and consolidate Service/Agency requirements for contract modifications; coordinate technical evaluations or proposed procurements; coordinate and direct contractual activities and represent the Joint Chiefs of Staff, when appropriate, in contract negotiations.

7. Coordinate with the WWMCCS ADP Logistic Support Panel, Services, and DoD Agencies regarding the Integrated Logistic Support Plan. Forward logistic support requirements and plans to the Single Service Logistics Manager through the Joint Chiefs of Staff.

8. Coordinate with the WWMCCS ADP Training Panel, Services, and DoD Agencies in determining WWMCCS and NATO training requirements and coordinate with the Single Service Training Manager to assure that WWMCCS training plans and programs meet requirements.

9. Coordinate and assist Services/Agencies with TEMPEST requirements and participate in equipment qualifications with the Successor Contracting Officer and the vendor.

10. As required, provide representation for the Joint Chiefs of Staff on Service/Agency-conducted on-site management surveys of WWMCCS ADP installations.

INFORMATION SYSTEMS DIVISION FUNCTIONS TRANSFERRED TO DCA

1. Provide technical management of the Unit Status and Identity Report (UNITREP) system, including:

a. Identifying and implementing design changes of the computer-based system to enhance economy and efficiency of operations.

b. Implementing system changes necessary to comply with OJCS policy.

c. Assisting system users and reporting agencies in the validation of data.

d. Responding to recurring and ad hoc OJCS requirements for reports of readiness, status, location, and personnel information provided by the system.

2. Act as the technical point of contact for worldwide subscribers regarding UNITREP software systems operation and capabilities.

3. Provide technical representation to applicable UNITREP system user and technical groups and committees, as appropriate.

4. Provide centralized technical management of assigned computer-based WWMCCS ADP Standard reference files (e.g., Geographical Location File (GEOFILE), Major Equipment Identification Code (MEQPT), Nicknames (NICKA), Unit Type Code File (TYPER)). Provide technical support to the OJCS for the development, maintenance, operations and dissemination of the files, including:

a. Insuring implementation of software changes necessary to enhance functional utilization and improve computer processing.

b. Assisting system users and reporting agencies in the validation of data.

c. Assisting OJCS users in file utilization.

d. Work in coordination with data managers in the development and standardization of reference codes identifying locations, unit identities, major equipments, and unit types in support of integrated reporting and computer processing procedures.

5. In coordination with the OJCS and the Services, provide technical management of the WWMCCS Standard Application Software Systems developed and projected for ADP support of the Joint Operation Planning System (JOPS) Volume III.

a. Act as the central technical point of contact for the OJCS and WWMCCS ADP community and the technical agencies providing direct technical support to the systems.

b. Maintain liaison with the agency responsible for functional management of the JOPS Volume III.

APPENDIX VI

BASIC PRINCIPLES OF INTERACTION BETWEEN THE C^2 ADP DIVISION OF JOINT C^3 AND DCA (CCTC)*

1. The Joint Staff will establish and provide guidance on overall program policy.

2. The Joint Staff will process requirements, prioritize, and validate them. These will be kept in a consolidated list and will be updated on a periodic basis.

3. On an annual basis, with periodic updates, the Joint Staff will forward the requirements to DCA (CCTC).

4. DCA(CCTC) and the Joint Staff will discuss these requirements and assess the basic technical, cost and schedule feasibility of implementing capabilities to support the established requirements.

5. After completion of the formal and informal discussions about the requirements, DCA (CCTC) will develop and forward to C^3 the annual program plans for the C^2 ADP program for coordination with the Joint Staff.

6. Formal coordination with the Joint Staff will occur on these plans.

7. Based upon agreement about the plan(s), the program (POM) will be developed and submitted by DCA (CCTC).

* Note these operating principles are also illustrated in the Diagram on the following page.

OVERVIEW OF JOINT C^3/DCA WORKING RELATIONSHIP

C^3 develops, coordinates, and publishes on an annual basis: 1) A consolidated, prioritized, validated set of requirements. 2) A limited set of functions, performance, research and development objectives.	Informal negotiations on technical, cost, and schedule feasibility of meeting requirements and achieving objectives.	DCA (CCTC) develops, coordinates, and publishes annual plans for C^2 ADP.	Review, comment on plans, reconcile differences.	DCA (CCTC) translates plan into POM.
ANNUAL PLANNING/PROGRAMMING CYCLE				
WHO IS INVOLVED				
C^3, CINC, Services with DCA (CCTC) advice and support	C^3 and DCA (CCTC)	DCA (CCTC) with C^3 coordination	Joint Staff and DCA (CCTC)	DCA (CCTC) with C^3 cognizance

- Indicates Product is produced.

APPENDIX VI

APPENDIX VI

PROPOSED LIST OF BILLETS TO BE
TRANSFERRED FROM THE OJCS TO DCA
AND
ASSOCIATED ADMINISTRATIVE ACTIONS

A. From the J-3, WWMCCS ADP Management Division

Title	Grade/Rank	OJCS Billet Number
Div Chief	Civ-GS-17	EB800010
Project Officer	A-05	EB803050
Project Officer	GS-15	EB803020
Branch Chief	N-06	EB804010
Project Officer	A-05	EB804020
Project Officer	N-05	EB804030
Project Officer	MC-05	EB804040

B. From the J-3, Information Systems Division

Title	Grade/Rank	OJCS Billet Number
Project Officer	N-05	EB203050
Project Officer	Civ-GS-14	EB203020
Computer System Superintendent	AF-E8	EB202050
Operations Systems Analyst, Operations Data NCO	AF-E7	EB202060
Programmer/Analyst, Operations NCO	A-E7	EB202070
Operations Systems Analyst	N-E7	EB202080

C. In conjunction with these personnel transfers, the following actions are required:

1. A transfer of the SI numbered billets for the transferred personnel.

2. A modification to the DoD High Grade Program to increase DCA's high grade ceiling by the number of spaces actually transferred.

3. A transfer of funds sufficient to cover civilian salaries, personnel support costs, and any other direct costs associated with the transfer.

4. A transfer of the Senior Executive Service space (resources) as allocated to former position of WWMCCS ADP Management Division Chief to DCA(CCTC) is effected to accommodate this action.