DOCUMENT RESUME

05637 - [B1025974]

Multilevel Computer Security Requirements of the World Wide Military Command and Control System (WWMCCS). LCD-78-106; B-163074. April 5, 1978. 10 pp.

Report to Secretary, Department of Defense; by Fred J. Shafer, Director, Logistics and Communications Div.

Issue Area: Military Preparedness Plans: Military Communications and Information Processing Needs (803); Automatic Data Processing (100); Federal Procurement of Goods and Services: Definition of Performance Requirements in Relation to Need of the Procuring Agency (1902).
Contact: Logistics and Communications Div.
Budget Function: National Defense: Department of Defense - Military (except procurement & contracts) (051); National Defense: Defense-related Activities (054).
Organization Concerned: Department of the Army; Department of the Air Force; Department of the Navy.
Congressional Relevance: House Committee on Armed Services; Senate Committee on Armed Services.

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. A followup review was conducted to determine whether the multilevel computer security requirements of WWMCCS were being properly provided for by the Department of Defense (DOD) and if Air Force efforts to solve this problem had been properly considered by DOD. At the time of the review, WWMCCS officials had not endorsed or supported Air Force efforts on multilevel computer security even though the Air Force had demonstrated a potential for resolving the shortcomings of WWMCCS software. However, the Air Force terminated its efforts to develop multilevel computer security because of insufficient financing. The Departments of the Army and Navy also have a need for multilevel security in their computerized systems and had been waiting for capabilities being developed by the Air Force. The apparent need for a multilevel security system and the lack of a concentrated effort to meet it, as well as cancellation of the Air Force program which showed promise of meeting this need, resulted from a lack of centralized responsibility and authority for development of a multilevel system. An office within the Office of the Secretary of Defense should be given budget authority and responsibility for: control of all computer security research and development in DOD; review and approval of computer security requirements for all three services; review and approval of all computer security specifications, methodologies, and procurements; and review and approval of all long-range plans for WWMCCS and the services. (RRS)

5974

UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

LOGISTICS AND COMMUNICATIONS DIVISION

B-163074

April 5, 1978

The Honorable
The Secretary of Defense

Dear Mr. Secretary:

We have recently completed a review of the multi-level computer security requirements of the World Wide Military Command and Control System (WWMCCS). Multi-level computer security enables users of the system, with different levels of access to classified information, to simultaneously share the same computer equipment (time-sharing) and be denied access to information for which they are not authorized. 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.

The need for multi-level computer security in the military has been recognized for some time. Multi-level security in computer systems is based upon the military need for maintaining different levels of access to classified information. Over the years, this need has been extensively studied and evaluated.

In June 1967, the Deputy Director of Defense Research and Engineering (for Administration, Evaluation and Management) requested that the Director of the Advanced Research Projects Agency (ARPA) form a task force to study and recommend hardware and software safeguards that would satisfactorily protect classified information in multi-access resource sharing computer systems.

Most recently, in a report dated February 18, 1977, issued by the Command, Control and Communications Panel, Subcommittee on Investigations of the House Committee on Armed Services, it was noted that there is a requirement for time-shared communications for the transmission of warning and intelligence data to the National Command Authorities and for the dissemination of their orders to operational forces. However, the Panel noted that there are computer security deficiencies in the WWMCCS software.

The Panel stated that although the existing physical and environmental controls are adequate to prevent unauthorized persons from obtaining classified information, reliance on these controls alone precludes effective computer internetting in a secure environment. Computer internetting is a way of linking computers together by data communication lines so that information can be exchanged between locations. Internetting is essential to WWMCCS's secure environment and to our Nation's military readiness capability. Multi-level computer security is essential to internetting.

PRIOR REVIEW OF WWMCCS MULTI-LEVEL COMPUTER SECURITY

In a letter report to your office (LCD-75-116), dated July 21, 1975, we noted that the computer supervisory or operating system software delivered with the WWMCCS computers--General Comprehensive Operating Supervisor (GCOS)--does not provide for, and cannot be made to provide for, the secure type of operations required by the WWMCCS community. The design and development of this software did not include any formal consideration of computer system security; therefore, the fundamental requirements for multi-level security within the WWMCCS computers had not been met. We urged the Department of Defense (DOD) to consider alternatives for satisfying users' security needs before final approval was granted for internetting the WWMCCS computers.

One of these alternatives was to upgrade the existing Honeywell computers, and to use the Multiplexed Information and Computing Service (MULTICS) operating system software that was then being used by the Air Force Data Services Center. Alternatively, the MULTICS technology could be developed for use on other brands of computers to enhance the prospects of competitively obtaining future computers for WWMCCS, with an improved multi-level security capability.

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

The Director of Telecommunications 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.

FOLLOW-UP REVIEW OF WWMCCS MULTI-LEVEL COMPUTER SECURITY

The purpose of our follow-up review was to determine whether the multi-level computer security requirements of WWMCCS were being properly provided for by DOD, and if Air Force efforts to solve this problem have been properly considered by DOD. The Air Force work in multi-level computer security was undertaken by the Electronic Systems Division, Air Force Systems Command.

At the time of this review, responsible officials for WWMCCS had not endorsed or supported Air Force efforts on multi-level computer security, even though the Air Force had demonstrated a potential for substantially resolving the shortcomings of WWMCCS-GCOS software. As a result, the WWMCCS computer systems are not directly supporting the Nation's command centers in a time-shared environment, as originally envisioned, and do not provide all the information needed to maintain our military readiness capabilities.

According to a senior DOD official, it is clear as we look at the kind of planning now required to be done to support contingency operations from a command and control standpoint that we must have a much better way of moving information from the various command centers, one to another. This official acknowledged that most of the intelligence and operations types of information are now in data bases in separate computers. However, the intelligence must be compartmented or separated, as in a multi-level security environment, in order to protect the source. In other words, multi-level security is required for effective internetting of intelligence and operations types of information.

Air Force multi-level computer security development effort

The MULTICS computer software used by the Air Force Data Services Center resulted, in part, from research and

development efforts by the Electronic Systems Division. The Air Force capability was developed to a point where time-sharing could be performed up to a top secret level in a controlled multi-level environment, when processing data with multi-user secure capabilities.

Although the WWMCCS community requires multi-level secure capabilities above the top secret level, this capability represented a significant step forward in the state-of-the-art for computer software because nothing like it existed anywhere else.

Subsequent to our July 1975 letter report to your office, the Air Force planned to terminate its efforts to develop multi-level computer security because of insufficient financing. The Air Force did terminate its effort, although it appeared to offer a possible solution to WWMCCS computer security and related problems. Over $9.1 million had been spent on this effort. We expressed our concern over this apparent termination in a letter to your office on April 20, 1976. The Director, Office of Telecommunications and Command and Control Systems, responded to this concern on June 10, 1976, and indicated that the Air Force planned to continue financial support for the development of multi-level security through fiscal year 1981.

On August 23, 1976, the Air Force Systems Command instructed the Electronic Systems Division to take action to terminate their multi-level security program during fiscal year 1977, as the Command did not have adequate financial resources to continue efforts in this area.

Through discussions with officials of the Air Staff, we learned that the decision to terminate the Division program was based on budgetary instructions, dated August 4, 1976, received from the Director of Defense Research and Engineering, now known as the Under Secretary of Defense for Research and Engineering. The Air Force was instructed to defer $1.3 million from the fiscal year 1977 research and development budget, which included the Division security program, and the program was terminated.

The Division high-technology team, which successfully pioneered research and development in multi-level security, was essentially disbanded. Some of the technology in this effort, relating to prototype, multi-level security applications on a minicomputer, is being used for application

development by the Advanced Research Projects Agency (ARPA). However, ARPA is not able to fully maintain continuity of this multi-level security program, because the Air Force disbanded the majority of the team with extensive experience in developing multi-level security capabilities in both large and small computer systems. Only a few members of the Air Force team are assigned to assist ARPA. ARPA's experience is apparently limited, in part, to capabilities in small computers. As a result, it could take ARPA several years to reach the same level of expertise with large computer systems as had already been achieved by the Air Force.

A DOD secure computer operating system is being developed by ARPA for a minicomputer, using an operating system that is compatible with the Bell Labs UNIX operating system. The target system is called the "DOD Secure UNIX," and is scheduled for operation by September 1979. ARPA is also utilizing related technology, developed at the University of California, as part of the basis for the DOD Secure UNIX.

During December 1976--4 months after the Air Force decided to terminate the Electronic Systems Division multi-level security program--the Information Processing Panel of the Air Force Scientific Advisory Board conducted a review to resolve the following questions on the need for multi-level security within computerized systems:

--Should the Air Force have a program in this area?

--If so, what form should it take?

--Should there be changes in the Air Force's present program to make it consistent with the answers to the first two questions?

The Panel responded that multi-level security is a problem which will become more and more important to the Air Force. The Panel suggested that action be taken to assure that necessary security technology is available when needed and that a mechanism is available for transferring this technology into Air Force systems.

In February 1977, the Acting Director of Defense Research and Engineering recommended that DOD develop a strong program in computer security technology. The Air Force was requested to prepare a plan of action for work in this area, with emphasis placed on multi-level security assurance.

During April 1977, the Air Force Systems Command was requested by its Headquarters to prepare a proposed plan of action for this multi-level security effort. The Electronic Systems Division submitted a proposed plan titled, "Phased Enhancements for Internal Computer Security," to enhance the security of Air Force computer systems through both in-house development projects and recommendations to industry to undertake such developments. The plan does not directly address large-scale general purpose computers, such as those used in WWMCCS. Rather, it addresses small segments of the problem with a goal of implementing better security capabilities as they are developed.

Multi-level security needs by other military services and WWMCCS

During this review, we learned that the Departments of the Army and Navy also have a need for multi-level security in their computerized systems. However, these services have been waiting for the capabilities being developed by the Air Force. In the meantime, they have been relying on the alternative approaches to the multi-level security problem; namely, use of dedicated systems, use of periods processing, and use of system-high operations for each security level of data being processed.

These are essentially the same techniques used in WWMCCS and generally involve the following procedures:

--Use of dedicated computers and separate data bases. A separate computer is used for each security level of data being processed, and the data base for each machine requires manual intervention for updating files.

--Use of 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.) is 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 that all individuals (as well as terminal areas and communications) are cleared for the highest level of information that could be processed on the system.

Studies have shown that each of these techniques is costly and does not provide the time-shared computer resources needed by the military services and WWMCCS.

Approach used to test the Prototype WWMCCS Intercomputer Network

During September 1976, DOD Joint Chiefs of Staff tested six internetted WWMCCS computer systems to determine, among other things, if such a network would be a viable solution for providing data to support command and control decisions. This test was performed system-high, whereby all individuals had security clearances equal to the highest security level of data being processed in the computerized network. Such an approach to multi-level security could provide ready access to classified data for many individuals that may not be authorized to have it, although they should have the necessary level of clearance. In addition, system-high relies upon techniques which are costly and inefficient.

According to an Air Force study prepared by Honeywell Information Systems, Inc., system-high does not allow simultaneous handling of information at several levels for users of different levels of clearance. In other words, system-high does not provide for effective multi-level security. Further, the WWMCCS-GCOS operating system cannot be made secure to prevent individuals from gaining access to information they are not authorized to have.

Thus, system-high operations unnecessarily increase the security clearance levels of the individuals concerned with designing, developing, operating, maintaining, and using a system operating in this mode. Further, all equipment, including terminals and communications facilities, must be cleared to the highest classification that a system can process.

CONCLUSIONS AND RECOMMENDATION

We believe 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 need for multi-level security seems to have been recognized for some time, as indicated by responses to our earlier letters, the results of various internal studies, a congressional study, and by our discussions with responsible officials. However, this program was allowed to lapse despite its potential, and its highly skilled development team disbanded. The need for multi-level security appears to have been addressed, in part, by the Air Force's multi-level security program.

We believe the apparent need and the lack of a concentrated effort to meet it, as well as cancellation of the Air Force program which showed promise of meeting this need, are results of no centralized responsibility and authority for the development of multi-level computer security in WWMCCS. Thus, we have two services--Army and Navy--waiting for completion of a cancelled Air Force program; the Director of Telecommunications and Command and Control Systems taking a favorable position on the program in 1975; and the Director of Defense Research and Engineering directing cancellation of the program which could have solved the problem.

There appears to be no central DOD control-and-review mechanism to coordinate and plan for an orderly development of multi-level security for the services and for WWMCCS.

Apparently, the Air Force and the Director of Defense Research and Engineering did not adequately recognize a need for multi-level security in WWMCCS, until after the multi-level security program in the Air Force was terminated. Moreover, until 1977, or over 5 years after the contract award for the computers, DOD had generally not expressed much interest in advancing the state-of-the-art in computer technology to a point where the original goals for the WWMCCS computer systems could be achieved.

With the existing substantial investment in computers for WWMCCS and the resulting concentration of critical data bases, we believe that to achieve the full required operational capability, responsible management officials should have considered all available ongoing research efforts to develop the security technology. We further believe that any additional DOD research and development on multi-level security should cover the security needs of all major systems in DOD, including WWMCCS.

Further, procuring computer systems for WWMCCS could be of limited value, because DOD has not adequately funded one of its most promising multi-level computer security programs and has essentially disbanded its team experienced in this subject. In effect, DOD has limited the number of potential solutions to its multi-level security problems. Since DOD will probably replace the WWMCCS computers sometime in the 1980s, it appears that plans should be made now to solve the multi-level security problems.

We recommend 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.

As you know, section 236 of the Legislative Reorganization Act of 1970 requires the head of a Federal agency to submit a written statement on actions taken on our recommendations to the House Committee on Government Operations and the Senate Committee on Governmental Affairs not later than 60 days after the date of the report and to the House and Senate Committees on Appropriations with the agency's first request for appppropriations made more than 60 days after the date of the report.

Copies of this report are being sent to the Chairmen, House and Senate Committees on Appropriations; the Chairman, House Committee on Government Operations; the Chairman, Senate Committee on Governmental Affairs; and the Chairmen, House and Senate Committees on Armed Services. Copies of this report are also being sent to the Secretaries of the Army, the Navy, and the Air Force, and the Chairman of the Joint Chiefs of Staff.

Sincerely yours,

Fred J. Shafer
Director