DEFENSE COMMUNICATIONS AGENCY

COMMAND AND CONTROL
TECHNICAL CENTER

WASHINGTON, D. C. 20301

STAT [redacted]

21 NOV 1977

IN REPLY
REFER TO: C423

MEMORANDUM FOR THE DEPUTY DIRECTOR FOR OPERATIONS (WWMCCS AND TELECOMMUNICATIONS), J-3, OJCS
ATTN: Project Manager, WWMCCS ADP Program

SUBJECT: WWMCCS ADP Security Program Plan

Reference: (a) MJCS 84-77, WWMCCS ADP Upgrade TA/CE, 28 Mar 77
(b) C423 Ltr, WWMCCS ADP Upgrade TA/CE, 26 Apr 77

1. By reference (a) OJCS tasked CCTC to submit for approval a research and development plan for implementing the investigation and evaluation of (1) secure GCOS-resident subsystems, and (2) secure microprocessor-based subsystems and/or mini-based front-ends. By reference (b) CCTC accepted the tasking.

2. CCTC submits herewith a comprehensive research and development plan for WWMCCS ADP security. The plan responds to reference (a), and, in addition, provides information on software security engineering, security monitoring and intercomputer network security activities. The project is described in a top-down fashion proceeding from the multi-level security objective to the sub-objectives of protection, assurance and assessment, and to the lower level component tasks of the project. The proposed project falls within the resource constraints established by the FY78 PDM. Provision is made for at least annual updating of the plan. Early acceptance of the plan will permit its timely execution.

1 Enclosure a/s

LUCIEN CAPONE, JR.
Rear Admiral, U. S. Navy
Director

Defense Communications Agency

Command and Control Technical Center

WWMCCS ADP Directorate

Security Branch

WWMCCS ADP SECURITY PROJECT PLAN

NOVEMBER 1977

PREPARED BY:

Thomas E Bozek

THOMAS E. BOZEK
Chief, Security Branch

APPROVED BY:

Marsden E. Champaign

MARSDEN E. CHAMPAIGN
Chief, Advanced Systems Division

APPROVED BY:

BIRTRUN S. KIDWELL, JR.
Colonel, USA
Deputy Director for WWMCCS ADP

APPROVED BY:

LUCIEN CAPONE, JR.
Rear Admiral, U. S. Navy
Director

TABLE OF CONTENTS

1.0 PROJECT OVERVIEW

1.1 General Description

WWMCCS ADP Systems must comply with Department of Defense security policy directives and regulations pertaining to the handling of classified material. This policy basically requires the three following conditions:

- No unauthorized disclosure of information;
- No unauthorized manipulation of information;
- No unauthorized denial of service.

The WWMCCS ADP systems, as presently configured, do not and cannot provide a base for achieving the WWMCCS ADP security objective of multi-level security.(1) Furthermore, the methods currently employed to cope with the security problem, i.e., periods processing and split systems, generate high overhead costs, and are poor and costly long-term answers to the WWMCCS ADP security problem.

This plan responds to the WWMCCS operational requirement for multilevel ADP security. Because the state-of-the-art in ADP security technology does not readily provide multilevel security, several options for improving WWMCCS ADP security are being pursued. These options are the subject of research and development. Other activities are being pursued to enhance the baseline computer system to make it a more suitable environment for satisfying security objectives. The general project strategy for the baseline computer system is to substantially reduce the vulnerability of these systems to misuse, and information theft and contamination. This strategy is extended beyond the baseline computer system to the evolving and growing WWMCCS ADP local and internetted environments.

The Security Project is structured in a top-down manner with three major thrusts directed to providing the desired level of ADP security. Protection provides the means to control access to system resources and limit the user's freedom in the system to only authorized activities. Assurance provides the means to determine that protection measures are working and continuously invoked, as well as a deterent to would-be system misuse and/or abuse. Assessment provides the means to build protection and assurance measures correctly and to evaluate their quality for the purposes of certification and accreditation.

(1) An Analysis of WWMCCS ADP Security: Vol.I - The New Standard System Hardware and Software (C), System Development Corporation, Jun 74.

This plan represents a view of WWMCCS ADP Systems developed after a long-term systems analysis. The analysis has searched, evaluated and projected a wide range of operational and security requirements, existing and emerging technologies, potential architectural solution alternatives, and weighed these with a heavy dose of rationality and pragmatism. The plan depicts an evolving and growing WWMCCS ADP capability that is more responsive to WWMCCS ADP user needs and is more secure.

The WWMCCS computer systems are secure as a result of extensive physical access controls, personnel security and administrative procedures. The purpose of this plan is to identify a course of action that improves the security protection in the computer systems themselves to the extent that rigid external computer security controls could be relaxed if desired. In this context, an acceptable level, or adequate security, refers only to the security directly provided by the computer system. The plan addresses the state of technology, specific objectives of WWMCCS ADP security research and development, and resources. Updates to this plan will be prepared annually at a minimun, or as major project changes occur.

1.2 Rationale

1.2.1 Requirements Assessment

Requirements for WWMCCS ADP security have been expressed in three major forms: WWMCCS Program Guidance, OJCS tasking of DCA and the WWMCCS Architect Reports. The Security Program Plan is designed to accommodate the needs expressed by these sources of requirements in a programmatic way.

1.2.1.1 Early WWMCCS Program Guidance

Early WWMCCS ADP Program Guidance identified the requirement for multilevel ADP security, multilevel ADP features associated with the standard data management system and configuration design criteria for security in an internetted computer environment.(1) The data management system was developed and implemented after the procurement of the Honeywell Series 6000 (H6000) computer systems designated AN-FYQ 65(V), hereinafter referred to as 65(V). Configuration design criteria for network security have evolved with the Prototype WWMCCS Intercomputer Network (PWIN) and projected technological advances. It was assumed that the WWMCCS ADP security requirements would be accommodated through a modest RDT&E program directed to the 65(V). Subsequent experience has

(1) A summary of WWMCCS ADP security guidance and directives is provided at Appendix A.

shown this not to be true.(1)

1.2.1.2 WWMCCS Program Management Office (PMO) Tasking

Several specific tasks have been based on a perceived need to have a system security measurement capability(2) , real-time surveillance capability (a subset of the more general WASSO station requirement)(3) , and technical assistance required to certify and accredit various security capabilities. In general, these requirements directly express a need for improved system evaluation and assessment techniques and improved system development methods and tools.

1.2.1.3 WWMCCS Architect Reports

The WWMCCS Architect Reports represent the most recent and comprehensive coverage of WWMCCS ADP requirements although they have not been formally validated. Security, continuity, flexibility, connectivity, availability and responsiveness are among the requirements addressed. The security and workload problems of the WWMCCS 65(V) systems are cited as among the areas where requirements have not been satisfied. In addition, the existence of only the single path to data (i.e., through the 65(V)) is cited as unresponsive to continuity, flexibility, connectivity, availability and distributed data base requirements.

1.2.1.4 Requirements Synthesis

The WWMCCS ADP operational needs for security were analyzed during the first and second years of the project.(4) The requirements analysis was a synthesis of formal documentation pertaining to WWMCCS ADP plans, operations, and security, as well as other information obtained through visits to a limited number of WWMCCS ADP components and other DoD organizations (e.g., NSA and DIA). The requirements were expressed as being in one of two categories. Functionality refers to what the user can do with the system. Integrity refers to the assurance that the system is complete and effective on a continuous basis. The following are the synthesized functional requirements for WWMCCS ADP security(5) :

(1) JTSA Tech. Bulletins 730S-19 dated 30 SEP 73 and 730S-20 dated 30 DEC 73, and Multilevel Secure ADP Systems for WWMCCS: TA/CE dated MAR 76.

(2) WWMCCS M-62-74, Statistical Data to Determine Inadvertant Risk of Disclosure, 1 FEB 74.

(3) WWMCCS M-774-73, WWMCCS ADP Security Monitoring Capability, 2 NOV 73 and SM-448-75, Establishment and Support of WWMCCS ADP Security Functions, 8 AUG 75.

(4) See Appendix C for Security Program history.

(5) Operational Requirements for WWMCCS ADP Security(FOUO), System Development Corporation, JUN 74.

o System access (in the sense of system usage) must not be restricted by clearance level or need to know of users.

o It must be possible to authorize the use of any of the resources of the system (including the network) to any user who has a valid need derived from duly assigned mission or function. Such resources include media for communicating with the system, languages, access modes, and data access means.

o Concurrent production and development work must be supported by the WWMCCS ADP.

o Any temporary or permanent limitation on or extension of system use (because of security or not) should be made known to the user before he submits a job to the system or initiates a terminal session.

o Many WWMCCS components require sharing of physical resources but not data resources, although this is true almost exclusively with groups of consumer users of the system. As a way of enabling separate but concurrent use of system resources, there is general need for and willingness to use a limited function secure system.

o The WWMCCS computer systems must accommodate a frequently changing variety of user access needs.

o The system must be flexible, especially as it involves changing external interfaces. There should be no limitation due to security on the sharing of central, duplicated or segmented data resources (e.g., distributed data base) among users of various component systems, the timely bulk transfer of sensitive data and programs between systems and among users, or directed user-to-user communication.

o Access control features for all member systems of the WWMCCS Intercomputer Network must be based on equivalent premises and provide equivalent capabilities.

o Security should not constrain the growth and performance of the system where such is required to handle new applications or uses or where such takes advantage of new technology which enables WWMCCS components to better accomplish its missions and perform its functions. However, with regard to system changes made for security reasons, unless the addition or modification of a security feature materially affects the way the system works or is applied (e.g., enabling the system to support a new customer set), the change should have minimum impact on throughput and response time.

o The ability to place data or physical resources in the system must not be limited by the type and degree of sensitivity of that resource. A corollary requirement is that data and physical resources must exist in the system in a natural manner. In other words, as perceived by the user, the manner of an object's existence in the system must not be distorted for security reasons.

o Security features should have little impact on the way a user uses the system. As much as possible, security features should be transparent to the user. Security events or features should not cause a break in a person's job or terminal session without an advance notice or a save-and-restore capability. Preemptive activity for security reasons should be minimized.

Given a system which estabishes and controls authorized sharing of system resources, there is a system integrity operational requirement to assure that such a system is complete and effective on a continuous basis. The following are the synthesized system integrity requirements for WWMCCS ADP security:

o Resource Integrity. Once an object resource exists in the system, its sensitivity and integrity must be preserved. The owner, manager or office of primary responsibility must be able to control and account for who may access the object and what may be done with the object once access is granted.

o Accreditation and Certification. The means for approving systems to operate in a given mode is recognized as a fundamental operational requirement at every WWMCCS component. In this regard, there is an existing need to (a) determine a threshold of acceptability (i.e., establish an acceptable level of risk, the attainment of which can be determined) and (b) assess the security status of a planned or operational system with respect to this threshold.

o Maintenance Monitoring. The system is expected to undergo change (e.g., the incorporation of new system releases), the process of which must be monitored to ensure no adverse effect on system integrity. In support of this requirement there is a need for acceptance-testing tools and methods for verifying the design and development of new systems and for ensuring the security of existing ones through all aspects of maintenance including regularly scheduled and unplanned start-up and shut-down. Moreover, the system must function with modular independence so that a change of one part of the system will not adversely affect other parts of the system or introduce new flaws into the system.

o ADP System Security Officer. It is generally recognized in the WWMCCS ADP community that a formally designated and authorized security officer is needed to monitor the system's security features. It may be considered an operational requirement that such an individual have (a) the necessary training and experience (e.g., that he understands and can debug systems software), (b) organizational clout in the sense of acting as the commander's surrogate in matters pertaining to ADP security, and (c) the necessary tools, methodology and staff to carry out his duties. With respect to his functions, there is a current need for him to perform security surveillance in order to detect, analyze and respond to system events which constitute or precipitate security violations.

1.2.2 Technology Assessment

The general concern for computer security has led to a number of attempts to assess the level of security in common general purpose computer systems such as the WWMCCS standard system. In general it has been found that these systems could not prevent skilled penetrators from subverting existing protective mechanisms and gaining the ability to access or change information within the computers. This was assessed as the result of a minimal concern for security in the original system development, a tendency to stress system performance over security, and the inability to ensure that a piece of software as complicated as an operating system performs correctly under all circumstances.

Such was the condition of these systems that retrofitting security into them was not feasible. Patches to implement corrections often only introduced new flaws. Moreover, even when implemented correctly, additional flaws elsewhere in the system, which also needed corrections, could always be identified. It was, therefore, reluctantly concluded that if security was not a serious goal of the initial development, then a system was unlikely to be secure or secureable for the multilevel mode of operation.

In the wake of these discoveries, a number of efforts were undertaken where security was a main consideration. However, to date such efforts have generally been limited to research or academic environments. Moreover, very limited systems have resulted because of the primary focus on the development of security technology. Such systems have proved of little utility in an actual operational environement.

Even where systems have been built to be both secure and useful to a wide community, the results have been mixed. Penetration tests on the most noteworthy of these systems, i.e., MULTICS, have shown that flaws have not been eliminated. However, it is believed that the basic design is sound and intuition indicates that what flaws do exist could be repaired. One caveat is that the time and resources required to reach this state were extensive. Another concerns the size and complexity of

Multics. Specifically, in its present state no formal or informal proof is possible to assure that the resulting system is secure. The only proof possible is that a skilled penetrator could find no flaws. Such a method has clear limitations particularly in a DoD environment.

A technique that does provide some level of security and also appears to be practical within the state of these technologies is compartmentation. With this scheme, users are grouped homogeneously by clearance level and each group is assigned to a system which is isolated from that used by other groups. This is, of course, the case with the separate systems and periods processing approaches to security. However, when these separate systems share some resource, a mechanism is needed to maintain isolation. If the mechanism required is sufficiently simple, it could potentially be built in a secure fashion using carefully applied software engineering techniques.

Compartmentation has two main manifestations. The first is a Virtual Machine Architecture where a set of pseudo-machines are created in software and share the real hardware through a mechansim called the Virtual Machine Monitor. The second is separate hardware systems which access a common resource through a common mechanism implemented in a separate hardware base. A network front-end providing access to a network for several separate systems at an individual site is an example of such a common mechanism.

There are a number of drawbacks to the compartmentation approach. First, within a compartment, no additional protection is provided between users than existed under the original system. However, since the threat is only from users of the same clearance level, it can be argued that the risk is within acceptable limits. A second drawback is that sharing between compartments has to be severely limited or else the sharing problem can essentially become as difficult as sharing in the general purpose operating system. Not all applications lend themselves to such restrictions. A final drawback is that building even these small mechanisms securely is still a topic of research and, moreover, not all hardware and software bases are amenable to this approach.

There is a final approach which has proved useful in some actual applications. In the approaches noted above, someone is required to develop at least a major piece of system software if not a whole operating system. A single user with a small number of his own applications does not generally want to take on a major system software or operating system development effort, as well as that associated with his own application. It is desirable to remain within the limits of the existing system. There is some hope that it is possible to build secure subsystems or applications on existing systems. Penetrators have noted that some capabilities, even under a basically unsecure operating system, cannot be subverted directly but only through other less secure capabilities. If only these impenetrable subsystems were configured into a particular system, the notion is that such a system would be secure. Moreover, a secure operating system would not be required.

This approach appears achievable and potentially at a relatively low cost. The problem is that not all subsystems lend themselves to this approach. It is believed, however, that the number of those subsystems that potentially do lend themselves to this approach can be expanded by care in the development process. A subsystem fitting in this category depends on the environment, the underlying hardware base, and the operating system as well as some inherent characteristic of the subsystem itself. Again, testing is the only approach to determining whether security has been attained. An understanding of the parameters of this approach are still a topic of research although, as noted, specific applications of it have met with some success.

Great strides have been made in the area of software engineering with such informal techniques as structured programming to the very formal technique of proof of correctness. These techniques promise eventually to provide the level of assurance of a system's security that is desired, i.e., multilevel ADP security. At present the application of formal techniques is limited by the size, complexity, and structure of the system to which they are applied. General purpose operating systems are believed to be at least on the fringes of the technology and more likely outside of it. However, by applying a balance of available and emerging software engineering techniques on a more limited basis, it appears technically feasible to substantially improve security in the WWMCCS ADP systems even though multilevel ADP security will likely not be achieved in the near future.

1.2.3 Operational Utility

The specific security and operational improvements that can be expected to result from the Security Program are:

o Functionality. The WWMCCS ADP Systems will provide end users (e.g., commanders; analysts) with expanded capabilities or opportunities of data collection, reduction, formatting and update facilities necessary for the effective performance of their duties.

o Performance. The WWMCCS ADP Systems will offer response times and through-put rates that are "natural" to the end user's job performance.

o Reliability. The WWMCCS ADP Systems will incorporate failsafe or failsoft modes to survive all anticipated emergencies or crises.

o Availability. The capabilities and qualities of the WWMCCS ADP system will grow in an evolutionary manner with emphasis on such factors as ease of conversion, degree of dependability, and extent of manageability.

o Cost. The WWMCCS ADP Systems will realize economies of resources with emphasis on the efficient use of and service for personnel, facilities, equipments, logistics, and technology.

It is expected that the operational needs are compatible with those for security, and that in many instances the fulfillment of one can act as a facilitating condition for another.

1.3 Project Strategy

1.3.1 Approach

The fundamental strategy of the Security Project is to systematically and incrementally reduce the vulnerability of the WWMCCS computers from system misuse, and information theft and contamination. The capabilities providing this vulnerability reduction will be implemented as part of the standard WWMCCS software releases. As a minimum, the criteria for demonstrating the quality of improvements in security will be extensive design and implementation review and testing.

The Security Project consists of three programmatic areas each corresponding to necessary conditions for ADP security. These project areas are protection, assurance and assessment. Protection is based on the principles of "least privilege" (i.e., grant a user only the smallest possible set of security and use privileges necessary to perform his assigned task) and "controlled access" (i.e., grant access to only that sensitive information for which the user has the appropriate access authorization and an established need-to-know). These principles, if perfectly implemented, would theoretically eliminate the vulnerability of the computer system from misuse, and information theft and contamination. The technical requirement that emerges from these principles is compartmentation of users, processes and information. Thus, it is necessary to be able to isolate users, processes and information in a controlled way to achieve the desired degree of computer security. Controlled sharing and controllable isolation are currently achieved via a closed environment with dedicated or split systems and periods processing.

Assurance provides demonstrations that security capabilities are operable and continuously invoked both on a scheduled and demand basis.

If the rationale for the two former program areas are sound, the thorny problem remains of whether or not the capabilities resulting from these strategies work correctly. Assessment attempts to formulate a rational set of approaches and solutions to the completeness/correctness problem. However, because the ideal technical solutions are beyond, or at least on the fringes of, the state-of-the-art, the degree of computer security that is adequate, i.e., internal computer security beyond that of physical, personnel and procedural measures) remains to be a difficult unresolved policy issue. The responsible authorities for WWMCCS ADP must ultimately make the policy decision of just what degree of computer security is "adequate". Determining the degree of security that is adequate requires risk assessment and a clear definition of the security requirements for WWMCCS ADP. In addition, the technical acceptance criteria for the degree of security that is adequate must be established as a matter of policy. The alternative is simply to accept whatever technical alternatives are made available.

Several considerations and assumptions are an implicit part of the Security Project strategy. They include:

a. Reliance on physical and procedural security measures. This will continue through FY81 as the basis for a "controlled environment", although a monotlithic environment (i.e., clearing everyone at the highest level) will become less tolerable.

b. 65(V)/GCOS III will remain the WWMCCS standard general purpose computer system through 1981.(1)

c. Although it will change in composition and character from its current status, PWIN will continue as the primary WWMCCS experimental network environment, evolving in its operational incarnation as a globally distributed computer network.

d. Other computer systems (e.g., HIS Level 6, DEC PDP11, HIS H700) will be used in the WWMCCS ADP community as special purpose processors.

e. The current trend toward greater use of transaction subsystems oriented to end-users (i.e., WWMCCS analysts and operators) will continue. The need for general programming capabilities will decrease in relative importance as an operational requirement of WWMCCS ADP, although the use of highlevel user languages will increase.

(1) MJCS 84-77, WWMCCS ADP Upgrade TA/CE, 28 Mar 77.

f. The network front-end processor (NFE) will evolve in two, overlapping stages. The first stage consists of providing a host with a network interface capability oriented toward AUTODIN II, given a standard host front-end protocol (HFP). A host would be able to "talk" to other hosts via the AUTODIN II communications network. The second stage consists of providing distributed system access mediation, either for a nodal network (i.e., a cluster of hosts and terminals at a WWMCCS site) or for a logical WWMCCS computer network (i.e., some collection of WWMCCS network subscribers based on similarities of access authorizations).

1.3.2 Technical Risk

The project is oriented to relatively low risk research and development, primarily advanced development and engineering development. As such, care must be exercised in setting objectives and defining low level project interdependencies in order to maintain the desired low risk posture.

In as much as possible, a condition for proceeding with one element in one area of the project shall not be (1) the success of another element in another area of the program, nor (2) the general availability of a product from another area of the project. For example, the development of a near term protection capability shall not be dependent upon the availability of formal verification technology. Such a dependency can only delay development, implementation and operational deployment of the near term capability.

2.0 PROJECT OBJECTIVES

2.1 Approach

The objectives of the Security Project are a derivative of WWMCCS ADP objectives and tasking directed to the DCA, and requirements derived from the WWMCCS ADP community. The WWMCCS security objectives and tasks that have been directed to DCA are summarized in Appendix A.

Multilevel security remains a mid-term objective of the WWMCCS ADP program.(1) A cursory analysis of security terminology indicates that there are several "multilevel's"; typically users, terminals and data. The Security Project assumes that the basic object in the system (i.e., data) is the focal point for directed activities. So that while controllable isolation of users, processes and data are all important, the data is of paramount interest.

The Security Project objectives are structured in a top-down format to facilitate review and analysis for consistency, completeness and project continuity. Two levels of objectives are specified:

2.1.1 Generic - Applicable to any comprehensive and complete ADP security program.(2)

2.1.2 WWMCCS Specific - Applicable to problems in the WWMCCS ADP environment having activities that constitute advanced and engineering development.

2.2 Level One Objectives

The primary objective of the Security Project is to provide multilevel sharing of data bases. There are three conditions that must exist to satisfy this objective. The first is protection. The protection condition must be applied to key parts of the ADP entity to ensure that users and processes are permitted access to, and manipulation and disposition of data in accordance with security policy. The assurance condition provides policing of protection features to be sure they are working as intended. Lastly, the assessment condition provides a means to develop capabilities according to predefined criteria and, in addition, to measure the quality or integrity of security capabilities (both protection and assurance measures).

(1) MJCS-84-77, WWMCCS ADP Upgrade TA/CE, 28 Mar 77.

(2) May be useful in the derivation of a DoD-wide ADP security program.

The specific project objectives at this level are:

2.2.1 PROTECTION - Develop methods for accomplishing the isolation of users and capabilities from data, and controlling access to data in the ADP environment.

The complete separation or isolation of users, processes and data theoretically provides absolute security. However, effective and secure use of information requires controllable isolation of users, processes and data, and controlled access by users and processes to other processes and data. The ability to isolate these elements in a controllable and deliberate way comprises the fundamental ADP security protection attribute.

This objective is applicable to both the local WWMCCS ADP installation environment and the global, or intercomputer network, environment. Effective means for controlling access to and sharing data will be developed. An extension of current controllable isolation practices (i.e., dedicated processing) will be developed to help ensure authorized separation of users into discrete processing entities and in the overall ADP environment.

2.2.2 ASSURANCE - Provide a means to detect, collect and report security related events in the ADP environment, and a facility for taking action on these events.

There is a need to provide effective and continuous awareness of the security system during its operational employment. This awareness constitutes a major deterant to accidental or deliberate misuse of the system. Presently, only the most sophisticated systems personnel are capable of effectively ensuring security awareness on an operational system. System security administrators should not be required to have this level of sophistication.

Assurance measures are generally of two types: auditing and surveillance. Auditing measures require no human intervention. Surveillance measures provide a security officer with the means to check at random intervals and on demand the security status of the system, and the manner in which the system is being used. Surveillance measures may provide the security officer with the capability to intervene in the operation of the system to modify the security privileges of users, the security attributes of the system or data, or to monitor activity not normally recorded via auditing measures.

2.2.3 ASSESSMENT - Develop strategies to guide and methods to support the development of security capabilities, and to evaluate and demonstrate the quality and integrity of those capabilities.

The key to bona-fide security solutions is the recognition of their quality and not necessarily their number. The measure of quality is an exceptionally difficult task. For different security problems, degrees of quality reflecting position in the system, security criticality and complexity issues further complicates the problem.

Three major areas of investigation are required. The first is a general purpose methodology for the development of new capabilities and a means to demonstrate their quality and integrity during the development process. The second is automated development and assessment tools that reduce or eliminate human error in the security capability production process as well as the time to certify and accredit these capabilities. The third is system security evaluation and maintenance techniques for existing capabilities.

2.3 WWMCCS Specific Objectives

2.3.1 Evolution of WWMCCS ADP

WWMCCS ADP is evolving into globally distributed processing centers as a result of successes in prototype WWMCCS intercomputer network (PWIN) experiments. It is also evolving into locally distributed processing elements as a result of message processing, intelligent terminal and mini-computer requirements. The combination of these evolutionary directions and security objectives appears to be complementary.

2.3.2 Protection

Investigations of potential secure general purpose computing environments (e.g., secure operating systems) have been deemed of too high a technical risk and/or too costly. Accordingly, a different tack will be pursued which focuses on providing controllable isolation on a micro-level instead of the macro-level. The hypothesis is that limited function capabilities (subsystems) can be developed to provide a large set of relatively small systems. Furthermore, that these subsystems can operate as secure entities within the larger unsecured system is possible. Two types of secure subsystems from a user viewpiont are identified. "Conduit subsystems" ensure that the user is directed only to the desired and authorized system capability or application. "Container subsystems" are at the logical end of a conduit. Container subsystems seize control of user actions and schedule authorized processes and/or access authorized data on his behalf.

2.3.2.1 Local Environment

The security protection objective for the local environment is to determine the viability of the secure subsystem concept for providing controlled sharing and controllable isolation. Secure subsystems in this context consist of two classes: host resident (65(V)) subsystems operating under an unsecure operating system (GCOS III) , and locally distributed subsystems (intelligent terminal, special purpose processor) operating in the larger site environment. Neither class must provide a general programming capability. Each has a well-defined set of processing functions which are interpreted by "canned" trusted processes.

2.3.2.1.1 The objective of 65(V) resident secure subsystem efforts is to develop and demonstrate a method for providing controlled sharing and controllable isolation through logical isolation of users within well-defined, authorized capability sets.

2.3.2.1.2 The objective of locally distributed subsystem architecture efforts is:

(1) To achieve a degree of multilevel ADP security by physically isolating well-defined, authorized user capability sets, data bases and terminals as part of the secure subsystem concept,

(2) To integrate a number of related subsystem development efforts into a total system capable of satisfying WWMCCS ADP security and functional objectives,

(3) To investigate and evaluate performance and reliability attributes resulting from locally distributed processing.

2.3.2.2 Internetted Environment .

The security protection objective for the global environment is to provide secure connectivity and interoperability between and among internetted systems, remote WWMCCS concentrators and users. To accomplish this objective, the major areas of access control, authorization, audit, surveillance, security officer controls and integrity checks will be investigated and evaluated as a minimum. In addition, other relevant research and development efforts, sponsored by other organizations, that foster achievement of the objective will be evaluated and/or supported to ensure compatability for possible WWMCCS network integration.

2.3.3 Assurance

Verifying that all security mechanisms and procedures are both continuously invoked and functioning properly represents the security assurance function (referred to as security monitoring). The Security Project focuses on providing automated assurance measures. The system may be monitored by the WASSO either on a transactional basis (referred to as auditing) or on a non-transactional basis (referred to as surveillance).

2.3.3.1 Auditing

The auditing objective is to provide a total, detailed historical log of all user transactions within the system. The log will:

- o Include access control parameters involved in each transaction

- o Permit the reconstruction of events surrounding unacticipated security events

- o Aid in the determination of a potential security violator's intentions

- o Be implemented in such a fashion that potential or actual security violations are identified and brought to the attention of the WASSO.

2.3.3.2 Surveillance

The surveillance objective is to determine the extent to which user activity can be examined on a non-transactional basis. In contrast to auditing, a random element is introduced which allows data to be gathered about a user or user process at any stage in its processing by the system. As such, surveillance measures should provide the WASSO with the means to detect potential abuse (characterized by the authorized user misusing resources to which he has overall legitimate access) and potential penetration (characterized by an unauthorized user gaining access to the system and succeeding in circumventing protection measures). Three specific techniques which together or in some combination may achieve the surveillance objective will be investigated and evaluated:

- o Performance related surveillance to detect abnormalities in system performance possibly related to unauthorized denial of service

- o Random examination of system statuses to determine validity of suspect user, terminal, or process activity

- o Precautionary assurance to randomly switch different copies of system modules having different code sequences to disguise the location of critical data and code.

2.3.4 Assessment

Assessment consists of project level technical efforts to guide or support the technical efforts of other tasks such that they succeed both individually and collectively. The area is referred to as security engineering because it deals with methods to construct, stress and evaluate purported or actual software security capabilities.

2.3.4.1 Security Development Guidelines

The objective of security development guidelines is to produce and refine a Secure Software Engineering Handbook which contains strategies and approaches for the development or improvement of ADP security in WWMCCS. The handbook is intended to be a fusion center for material generated by the various efforts of the Security Project to include representative concepts of operations, design and development methodologies and specifications, testing and integration methodologies, deployment approaches, and operational maintenance procedures.

2.3.4.2 Security Engineering Tool Development and Integration

The objective of security engineering tool development and integration is to produce a comprehensive set of tools and technniques that facilitate the planning, performance and control of system security development processes. These tools and techniques shall impart a development discipline that ensures (a) the certifiability of selected system components, (b) the certifiability of the total integrated system, and (c) the cost effective application of system development or improvement efforts.

2.3.4.3 System Security Evaluation and Maintenance

The objective of system security evaluation and maintenance is:

2.3.4.3.1 To produce and refine a strategy and a specific set of tools and techniques for the certification and accreditation of the WWMCCS ADP system and its components.

2.3.4.3.2 To produce a set of techniques and tools that enable or facilitate WWMCCS ADP system engineers to perform operational maintenance in such a manner that (a) security related problems can be readily identified and eliminated, and (b) operational problems, including the normal system evolution, can be handled without adversely affecting the system security and integrity.

3.0 TECHNICAL DEVELOPMENTS ACTIVITIES

The technical developments of the Security Project are structured into four task areas: secure subsystems, security engineering, security monitoring and network security. These tasks correspond to the budget process project/task issue sheet structure. The network security task has been separated out of the secure subsystems task for visibility and clarity purposes.

Tasks are composed of one or more subtasks each responding in a particular way to the heirarhical set of program objectives. The task level/budget correspondence is:

		Task Number	
Program Objective	Technical Developments	RDT&E	O&M
Protection	Secure Subsystems (local)	4727301	1727301
	Network Security (global)	4727304	1727304
Assurance	Security Monitoring	4727303	1727303
Assessment	Security Engineering	4727302	1727302

Task level planning information is presented to permit easy update. The master copy will be maintained in loose-leaf form. The structure and paging scheme is as follows:

(____)

Task Description:

Subtask Interrelatinships:

Resources:

Schedule:

3:Task no.:Subtask no.:Subtask page no.

(____)

Subtask Objective:

Subtask Description:

Scope:

Issues:

Resources:

Schedule:

3:Task no.:Subtask no.:Subtask page no.

Resources:

RDT&E $K	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
3.1 Secure Subsystems	800	1050	1476	1694	1830	2032	8882
3.2 Security Engineering	400	450	250	250	300	300	1950
3.3 Security Monitoring	327	335	250	150	-	-	1062
3.4 Network Security	436	375	300	300	300	300	2011
TOTAL	1963	2210	2276	2394	2430	2632	13905

O&M $K	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
3.1 Secure Subsystems	95	100	78	90	154	189	706
3.2 Security Engineering	-	68	62	50	100	150	430
3.3 Security Monitoring	55	132	169	178	74	-	608
3.4 Network Security	-	-	-	-	-	-	-
TOTAL	150	300	309	318	328	339	1744

No procurement funds are programmed. Six (6) man-years per year are programmed except for Data Base Machine activity. Man power is accounted for separately for this activity.

3.1 Secure Subsystems

3.1.1 Description

Secure subsystems provide the security protection mechanisms in the local WWMCCS ADP environment. The two types of secure subsystems include conduits and containers. Conduit subsystems ensure that the user is directed only to the desired and authorized system capability or application. At the end of a series of conduits are container subsystems which seize control of user actions and schedule authorized processes and/or access authorized data on behalf of the user. Host-resident (65(V)) subsystems operating on an unsecure operating system (GCOS III), and locally distributed subsystems (e.g., data base machine, intelligent terminals) operating in the larger site environment will be developed. Limited improvements to GCOS III will be evaluated to determine if a more suitable secure subsystems environment can be provided.

3.1.2 Subtask Interrelationships

The secure subsystems concept provides a building block approach to system security within an overall system security framework. By describing the total system in terms of functional entities, functions may be added to or deleted from the total system permitting controlled and planned growth of the total system. Security is provided via the individual functional entities in the system. Each function is responsible for (1) containing the user within that subsystem, (2) limiting use within the subsystem only to actions specifically authorized, and (3) verifying the users authority to exit from the subsystem to another subsystem.

3.1.2.1 65(V)/GCOS III Subsystems

In the 65(V)/GCOS III context, secure subsystems would limit a user's freedom within the system to authorized functions. Currently, all users have complete freedom of the system. The limitation of user freedom (i.e., controllable isolation) begins at access time in the logon procedure. The logon procedure would capture the user and validate his authorization to use not only the computer system, but also the requested subsystem(s). When this authorization is validated, control of the user is passed to the subsystem. This procedure is continued through successive "conduit" subsystems until the target "container" subsystem is reached. At this point, the container subsystem acts only as an interpreter of user interaction and does not pass control of the user to the next level of system implementation (e.g., operating system I/O).

Two major issues are to be resolved in the investigation and evaluation of the secure subsystems concept in the 65(V). The first issue is whether or not the unsecure GCOS III operating system can be sufficiently improved from a system integrity standpoint to provide an acceptable environment for secure subsystems. The second issue will be addressed concurrently with the first. It will determine the security benefit that may be derived directly from secure subsystems. Two subsystems will be initially developed, one to provide an experimental baseline for a multi-user conduit subsystem. A second subsystem will be developed to provide an experimental baseline for a container subsystem. Security software engineering technology will be used to the maximum extent practicable provided the use of the technology is well-understood and does not significantly increase the technical risk of the effort.

3.1.2.2 WWMCCS Nodal Network

The development of locally distributed subsystems is a long term effort. The approach is to remove from the host computer or develop new functional capabilities placing them in discrete but interconnected intelligent processing units (e.g., mini-computers and intelligent terminals) comprising a network of computers at the local installation. Because WWMCCS ADP is evolving to this environment with the develpment of intelligent terminals and executive aids, it is imperative that the security aspects of this evolution be planned. The data base machine (DBM) is the first major subsystem to be specifically pursued in this evolving architecture. It would provide, in concept, the opportunity to isolate the data base from the unsecure host and to experiment with control features that would permit multilevel cleared users authorized access to the multilevel data base. In a colateral effort, alternative control structures will be formulated and evaluated which facilitate security, connectivity and planned growth in the nodal network.

Originating Objective: 2.3.2.1.1 AOD:
Budget Designator: 4727301 Priority:
Subtask Title: Secure Transaction Processing Executive (STPE)

Subtask Objective: To control and monitor the authorized user entering the 65(V) transaction processing environment and his access to authorized applications programs.

Subtask Description: The STPE is the experimental subsystem selected to accomplish objective 2.3.2.1.1. It will provide a secure conduit that passes user transactions and messages between terminals and autonomous applications programs (TPAPS) running under GCOS III, or between two or more such programs. In addition, the STPE will accommodate the operational environment currently served by the Navy TPE.

Scope: The functions to be provided by the STPE will be limited to Navy TPE functions (WWMCCS ADP TPE functions) supplemented by functions which improve functionality, enhance security and can be provided without major development perturbations.

Issues: Several issues are addressed by this subtask. The major issues are:

a. To determine the feasibility of secure subsystems in the general case, and of 65(V)/GCOS III conduit subsystems in the specific case.

b. To determine:

1. The nature of security policy that can be implemented by secure 65(V) conduit subsystems

2. The security functions with respect to (a) user access control and (b) subordinate conduit/container subsystems that must be implemented

3. The subsystem-operating system interfaces

4. The user interface to the secure subsystem and the richness of the user capability set.

c. To determine what must be done to the transaction processing environment to arrive at a secure transaction processing system.

d. To determine the feasibility of formal verification for large software subsystems development.

Originating Objective: 2.3.2.1.1 AOD:
Budget Designator: 4727301 Priority:
Subtask Title: Secure Transaction Processing Executive (STPE)

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	9	6	7	-	-	-	22
B. RDT&E $K	420	421	276	-	-	-	1117
C. O&M $K	-	-	60	90	-	-	150
D. Procurement $K	-	-	-	-	-	-	-
TOTAL	420	421	336	90	-	-	1267

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART

TITLE WWMCCS ADP SECURITY PROJECT PLAN
Secure Transaction Processing Executive (STPE)

CLASSIFICATION UNCLASSIFIED

AS OF DATE 1 NOVEMBER 1977

ITEM NO.	MAJOR MILESTONES	FY78			FY79				FY80				FY81				FY82				FY83				
		2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q
	STPE Security Model	△																							
	Formal Specifications				△																				
	Test/Evaluation Plan			△																					
	Initial Implementation						△																		
	T&E and Enhancement								△																
	Release to Sites/Maintenance										△														

Originating Objective: 2.3.2.1.2 AOD:
Budget Designator: 4727301 Priority:
Subtask Title: Experimental WWMCCS Nodal Network (EWNN)

Subtask Objective:

(1) To achieve a degree of multilevel ADP security by physically isolating well-defined, authorized user capability sets, data bases and terminals as part of the secure subsystem concept,

(2) To integrate a number of related subsystem development efforts into a total system capable of satisfying WWMCCS ADP security and functional objectives,

(3) To investigate and evaluate performance and reliabiliiy attributes resulting from locally distributed processing.

Subtask Description: The EWNN is the concept selected to accomplish objective 2.3.2.1.2. The concept provides the recognition that WWMCCS ADP is evolving into sets of processing components in the local installation environment. The 65(V) is a major processing component. In addition, the concept provides system integration which permits greatly improved security, configuration growth, and enforces standardization so that components are added according to pré-defined conditions. Architectural alternatives will be studied and a suitable mode of interconnection will be defined, along with a control structure and intra-site communication protocols. Functional and security specifications will be prepared, and an experimental system designed and developed, and experiments conducted in an operational environment to determine suitability for implementation as an operational capability. A 65(V), prototype data base machine, WASSO station and secure network front-end processor will be interconnected at a minimum.

Scope: The EWNN will be limited in terms of configuration to projected component (hardware and software) requirements for WWMCCS ADP. The EWNN will exploit and adapt distributed processing technology for the purposes of determining its usefulness for satisfying emerging WWMCCS ADP needs. Usefulness in this context will include security, opportunities for expansion of functionality, controlled configuration growth and evolution, availabilty, continuity and consistency with the WWMCCS System Engineer's Office (WSEO) plans and developments.

Issues:

The primary issue to be resolved is the determination and selection of an interconnect scheme with protocols and interfaces which support required security mechanisms.

Originating Objective: 2.3.2.1.2 AOD:
Budget Designator: 4727301 Priority:
Subtask Title: Experimental WWMCCS Nodal Network (EWNN)

Secondary issues include the verifiability of a distributed processing system, bandwidth limitations and cost/performance issues.

Originating Objective: 2.3.2.1.2
Budget Designator: 4727301
Subtask Title: Experimental WWMCCS Nodal Network (EWNN)

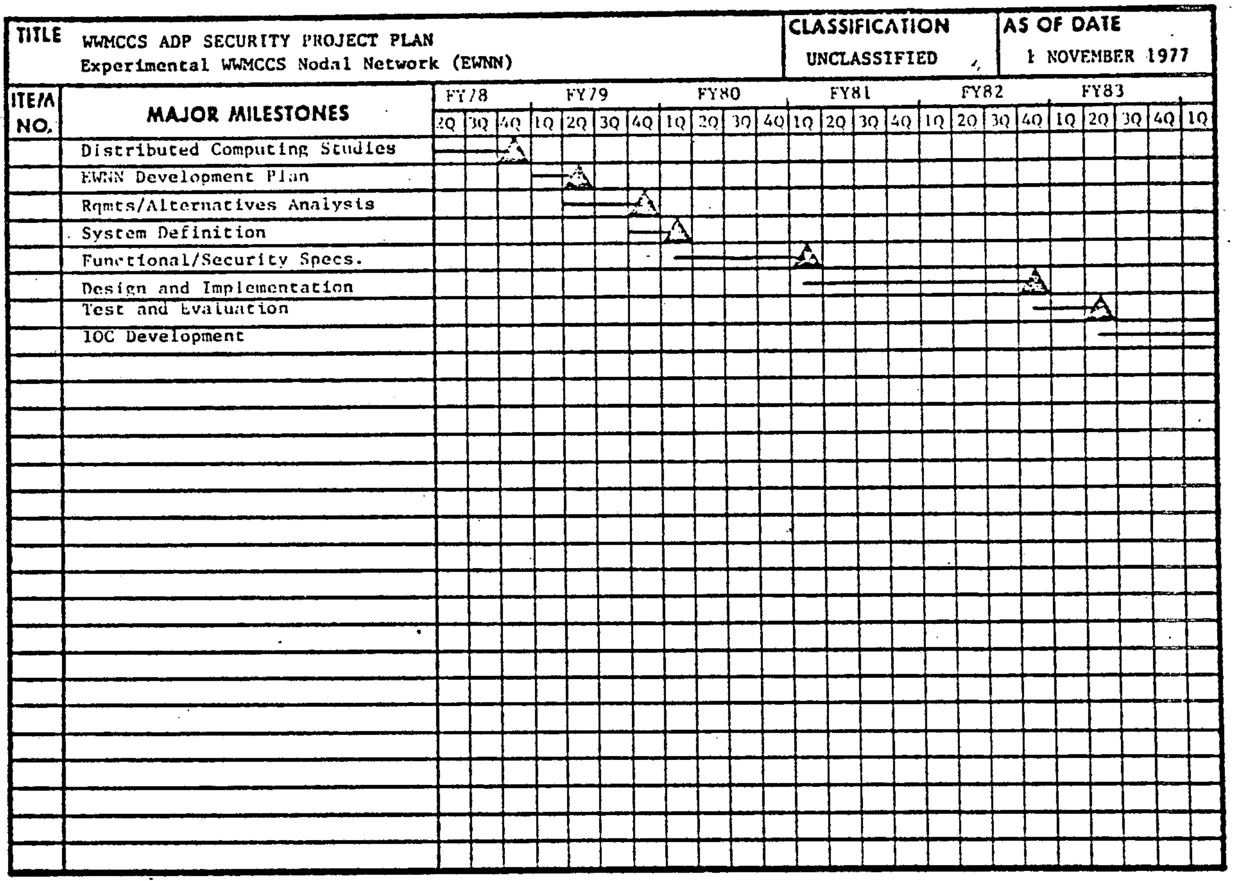
AOD:
Priority:

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	3	9	18	28	36	41	135
B. RDT&E $K	130	529	1200	1694	1830	2032	7415
C. O&M $K	-	-	-	-	154	189	343
D. Procurement $K	-	-	-	-	-	-	-
TOTAL	130	529	1200	1694	1984	2221	7758

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART



TITLE WWMCCS ADP SECURITY PROJECT PLAN
Experimental WWMCCS Nodal Network (EWNN)

CLASSIFICATION UNCLASSIFIED

AS OF DATE 1 NOVEMBER 1977

Originating Objective: 2.3.2.1.1 AOD:
Budget Designator: 4727301 Priority:
Subtask Title: Secure WWDMS Interface Software Package (WISP)

Subtask Objective: To demonstrate, in the very near term, the viability of 65(V)-resident secure subsystems by providing a secure user interface to WWDMS.

Subtask Description: WISP is a small, functionally limited GCOS III container subsystem designed to provide a simplified user interface to the WWMCCS data management system (WWDMS). It is currently a collection of time-sharing routines, transaction constructor (TCON) table generator statements, and new assembly language routines. It is intended to provide assurance that (a) users can only access individually authorized WWDMS procedures in a WISP library, and (b) procedures accessed and activated by WISP can only perform the limited functions for which they were written.

Scope: This subtask will (1) examine the WISP subsystem for security, functional and user-level deficiencies, (2) identify an approach and the level of effort required for certification, and (3) implement changes required to provide the required level of security and correct other deficiencies.

Issues: Two major issues are addressed by this subtask. The first is to determine the feasibility of on-line time-sharing container subsystems. The second is, for existing capabilities, determine the security characteristics required for the user's interface to data management functions.

Originating Objective: 2.3.2.1.1 AOD:
Budget Designator: 4727301 Priority:
Subtask Title: Secure WWDMS Interface Software Package (WISP)

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	4	1	-	-	-	-	5
B. RDT&E $K	150	-	-	-	-	-	150
C. O&M $K	45	25	-	-	-	-	70
D. Procurement $K							
TOTAL	195	25	-	-	-	-	220

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART

TITLE WWMCCS ADP SECURITY PROJECT PLAN
Secure WWMDS Interface Software Package (WISP)

CLASSIFICATION UNCLASSIFIED

AS OF DATE 1 NOVEMBER 1977

ITEM NO.	MAJOR MILESTONES	FY78			FY79				FY80				FY81				FY82				FY83				
		2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q
	Design and Implementation	—	—	△																					
	Test and Evaluation			—	—	△																			
	Release to Sites/Maintenance					△																			

Originating Objective: 2.3.2.1.1 AOD:
Budget Designator: 1727301 Priority:
Subtask Title: 65(V)/GCOS III Security Improvements

Subtask Objective: To provide a GCOS III system baseline environment suitable for host-resident secure subsystems.

Subtask Description: The GCOS III security improvements effort will raise the general level of system software integrity in order to make it more difficult for the noncompartmented (non secure subsystem) user to intentionally or unintentionally abuse his intended domain of authorization as represented by his explicit access privileges or permissions. Initial efforts will be directed at (1) the logon/authentication process particularly with regard to system release 7.1, (2) internal GCOS III interfaces, and (3) intersubsystem controls that regulate the sharing of a data base among two or more user subsystems that in turn regulate the exchange of messages among selected user subsystems. Additional effort will analyze and evaluate system deficiencies and determine the benefits of potential solutions.

Scope: This subtask is intended to raise the level of integrity of system software in WWMCCS host computers. It is not an attempt to make GCOS III secure.

Issues:

The first issue is whether or not key parts of GCOS III can be redesigned and/or reimplemented in such a way that the integrity of the system can be sufficiently improved to provide a suitable environment for secure 65(V) subsystems.

A second issue is what constitutes a suitable secure subsystem environment.

The third issue is what constitutes encapsulation of a set (subset) of functionally unique users.

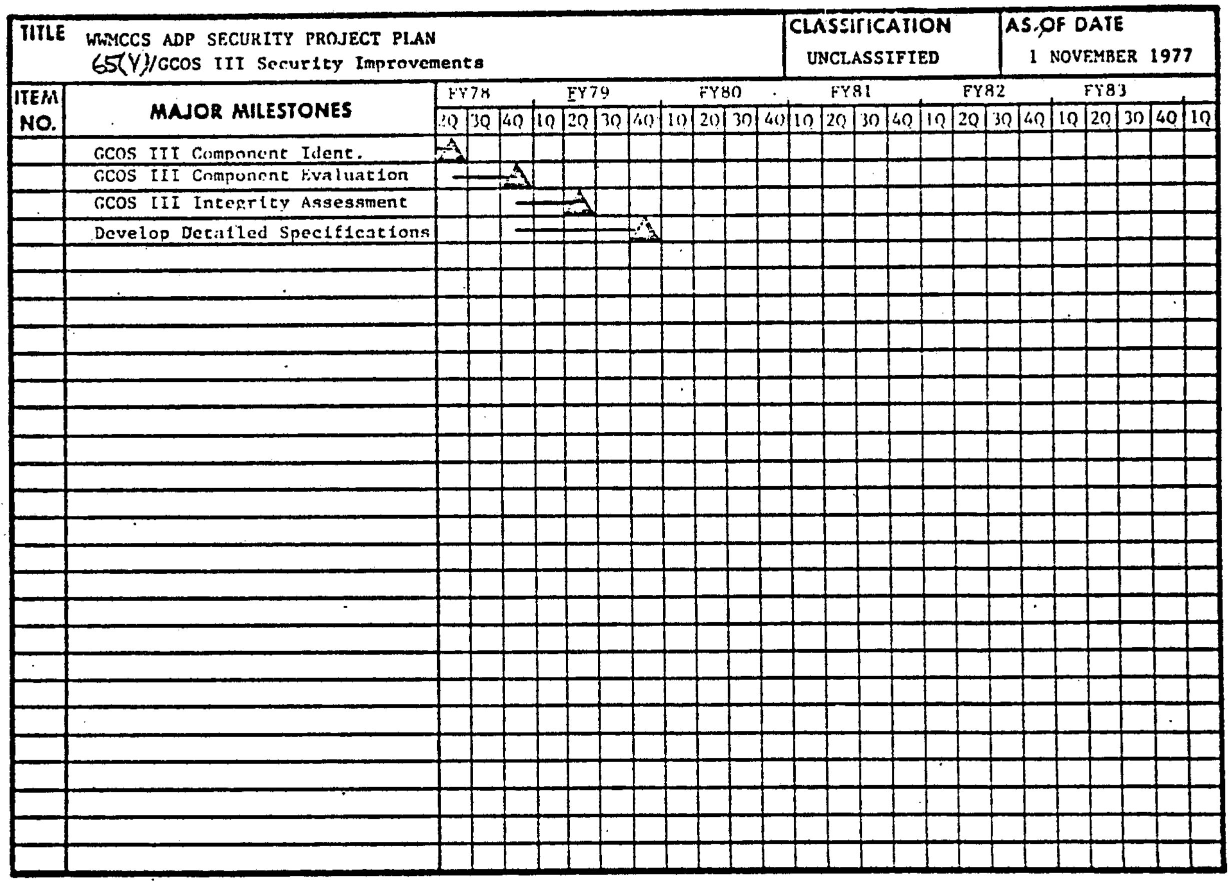
Originating Objective: 2.3.2.1.1	AOD:
Budget Designator: 1727301	Priority:
Subtask Title: 65(V)/GCOS III Security Improvements	

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	2	1	-	-	-		3
B. RDT&E $K	-	-	-	-	-	-	-
C. O&M $K	50	75	-	-	-	-	125
D. Procurement $K	-	-	-	-	-	-	-
TOTAL	50	75	-	-	-	-	125

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART



TITLE WWMCCS ADP SECURITY PROJECT PLAN
65(V)/GCOS III Security Improvements

CLASSIFICATION UNCLASSIFIED

AS OF DATE 1 NOVEMBER 1977

ITEM NO.

MAJOR MILESTONES

- GCOS III Component Ident.
- GCOS III Component Evaluation
- GCOS III Integrity Assessment
- Develop Detailed Specifications

Originating Objective: 2.3.2.1.1 AOD:
Budget Designator: 4727301 Priority:
Subtask Title: Secure Transaction Processing Application Program (STPAP)

Subtask Objective: To develop and demonstrate the containment of the TPAP user within the authorized functional capabilities of the TPAP.

Subtask Description: An STPAP will be developed to demonstrate the technology and method for such container subsystems. Initially, an analysis of the existing TPAPs will be conducted to select a representative TPAP based on TPAP functionality, and user-TPAP, TPAP-TPAP, and TPAP-system interfaces. The demonstration of the STPAP and the secure transaction processing executive will serve as a baseline secure transaction processing system.

Scope: This subtask will be limited to the develoment of one representative secure transaction processing application program. The technology and method of develpment, as well as a security demonstration, will be exported to the WWMCCS ADP community for use by the community.

Issues: The major issues to be addressed by this subtask are:

a. to determine the technical feasibility of developing STPAPs and a secure transaction processing system.

b. to determine the feasibility of exploiting this method for the development of operational transaction processing systems by the WWMCCS ADP community.

Originating Objective: 2.3.2.1.1
Budget Designator: 4727301
Subtask Title: Secure Transaction Processing Application Program (STPAP)

AOD:
Priority:

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	2	3	-	-	-	-	5
B. RDT&E $K	100	100	-	-	-	-	200
C. O&M $K	-	-	18	-	-	-	18
D. Procurement	-	-	-	-	-	-	-
TOTAL	100	100	18	-	-	-	218

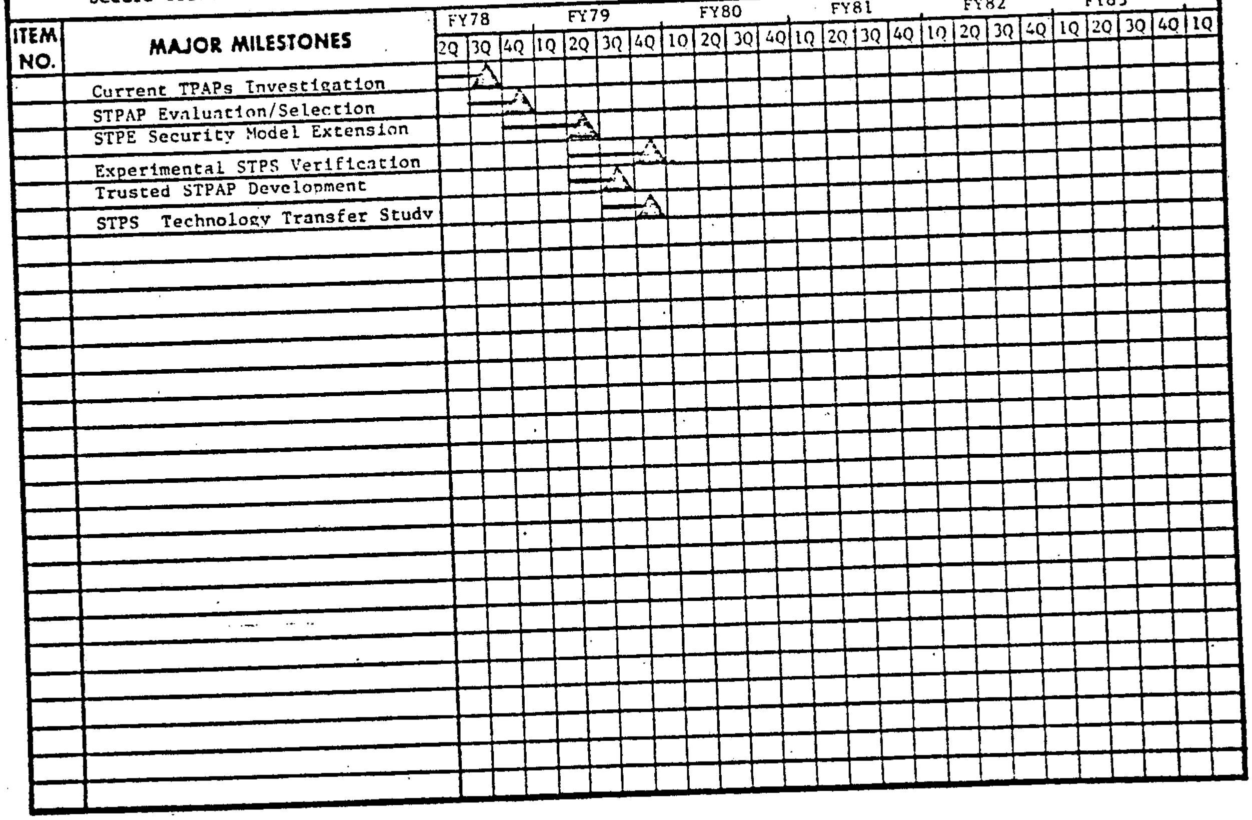
Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART

TITLE WWMCCS ADP SECURITY PROJECT PLAN
Secure Transaction Processing Application Program (STPAP)

CLASSIFICATION UNCLASSIFIED

AS OF DATE 1 NOVEMBER 1977



Originating Objective: 2.3.2.1.2
Budget Designator: 4727401
Subtask Title: Data Base Machine

AOD:
Priority:

Subtask Objective: To develop specifications for an enhancement to the current WWMCCS ADP data management capabilities that will provide for the secure sharing of data at various levels of classification between computer systems operating at different security levels.

Subtask Description: The DBM development is a five phase effort culminating in the specificcation of an operational WWMCCS DBM. The first phase of the effort, which has been completed, is the concept formulation and feasibility phase. This phase was used to identify the basic attributes of a WWMCCS DBM and evaluate alternate research approaches for its development. Phase two will define modes of operation, performance profiles, and functional specifications. Phase three will provide design specifications and a TA/CE for Service/Agency concurrences. Phase four will constitute the development of a prototype DBM based upon the results of prior phases. This phase will include experiments to validate, and modifications to optimize the prototype. The final output of this phase is a functional specification for a WWMCCS DBM. Phase five will deal with obtaining Service/Agency concurrences with the WWMCCS DBM specifications.

Scope: The DBM will retain WWDMS capabilities. It will be demonstrably capable of enhancing WWMCCS ADP security. Specific effort will be pursued to try to minimize additional performance degradation. The implementation of a WWMCCS DBM should impose little or no conversion requirements for current WWMCCS ADP systems.

Issues: Five major DBM issues will be addressed:

a. Determine the extent of security policy control and enforcement possible via the DBM

b. Determine the security policy to be implemented in the DBM for WWMCCS multilevel security

c. Determine the relationship of the DBMto WASSO and data base administrator functions

d. Certification of DBM software.

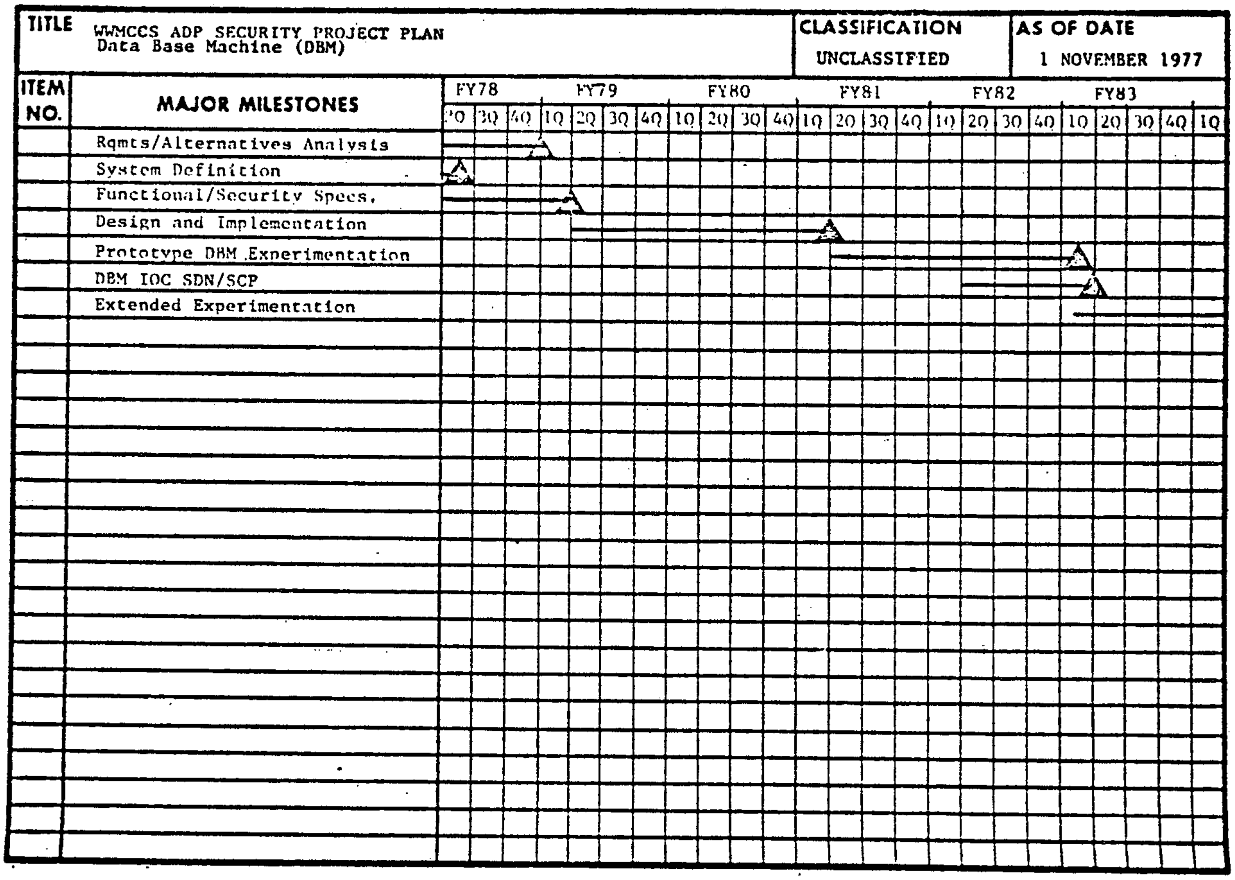
Originating Objective: 2.3.2.1.2	AOD:
Budget Designator: 4727401	Priority:
Subtask Title: Data Base Machine	

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	8	12	24	24	24	24	116
B. RDT&E $K	250	500	500	500	500	450	2700
C. O&M $K	-	-	-	-	-	-	-
D. Procurement	-	-	-	-	-	-	-
TOTAL	250	500	500	500	500	450	2700

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART



3.2 Security Engineering

3.2.1 Description

Security engineering consists of project level technical efforts which guide or support the technical efforts of other tasks such that they succeed both individually and collectively. It deals with the methods and tools to construct, stress and evaluate software security capabilities. The three major thrusts of this task are (1) to produce and refine a Secure Software Engineering Handbook that contains strategies and approaches for the development and improvement of ADP security in WWMCCS, (2) to produce a comprehensive set of tools and techniques to facilitate the planning, performance and control of system security development processes, and (3) to produce and refine system security evaluation and maintenance methods and tools to support the approval of security software and facilitate its credibility during maintenance.

3.2.2 Subtask Integration

The security engineering concept provides a disciplined approach to the design, development, certification and maintenance of secure software. It prescribes methodologies for the production of certifiable systems and provides an environment with tools to support these methodologies. It will apply modern software engineering principles for producing highly reliable programs and make available a set of automated tools for enforcing or supporting these principles. The security engineering task consists of three subtasks which correspond to the higher level objectives of the security program. These include: (1) a secure software engineering handbook, (2) tools which support software production, and (3) tools which support security certification and maintenance.

Originating Objective: 2.3.4.1 AOD:
Budget Designator: 4727302 Priority:
Subtask Title: System Security Engineering Handbook

Subtask Objective: To produce a handbook which will assist the WWMCCS ADP Directorate, WWMCCS site commanders and configuration managers, and WWMCCS support contractors in developing highly reliable and trusted software. It will, in particular, aid in the production of functional software packages, subsystems and systems which must be designed and certified for enforcement of or compliance with security policies and regulations.

Subtask Description: This subtask will be directed toward the preparation of a handbook which describes (1) the approved security modes under which WWMCCS systems can be operated, (2) the procedures in use in WWMCCS for achieving ADP security, (3) the degree of software verification required for the various security modes, (4) the range of verification techniques needed for certification, and (5) specific software engineering methods, techniques and tools which should be utilized to facilitate certification.

Scope:

The handbook will be a management-oriented document which assists in selecting appropriate develoment methodologies, techniques and tools for producing and verifying WWMCCS software which must be certified against criteria based on its criticality in its functional environment and the reliance placed on it to enforce security policies and regulations.

The handbook must be organized in a logical, coherent manner with emphasis placed on those project management aspects of trusted software development which result in the application of appropriate methods, techniques and tools for a given degree of security.

The guidelines presented in the handbook should apply the concepts developed, facts uncovered and lessons learned in the course of the research conducted by the Security Project and supplemented by the results of other pertinent studies.

Issues:

The primary issue to be resolved is thc degree of software verification required for each of the various security modes under which WWMCCS ADP systems can be operated.

A secondary issue is the cost/benefit tradeoff associated with assuring the desired level of security.

Originating Objective: 2.3.4.1
Budget Designator: 4727302
Subtask Title: System Security Engineering Handbook

AOD:
Priority:

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	3	3	2	2	2	2	14
B. RDT&E $K	33	-	-	-	-	-	33
C. O&M $K	-	-	-	-	-	-	-
D. Procurement $K	-	-	-	-	-	-	-
TOTAL	33	-	-	-	-	-	33

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART

TITLE	CLASSIFICATION	AS OF DATE
WWMCCS ADP SECURITY PROJECT PLAN System Security Engineering Handbook	UNCLASSIFIED	1 NOVEMBER 1977

ITEM NO.	MAJOR MILESTONES	FY78			FY79				FY80				FY81				FY82				FY83				
		2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q
	Problem Definition/Analysis	▲																							
	Handbook - Initial Version	▲																							
	OJCS Approval		▲																						
	Release to Sites		▲																						
	Handbook - Revisions				▲			▲				▲				▲				▲				▲	

Originating Objective: 2.3.4.2 AOD:
Budget Designator: 4727302 Priority:
Subtask Title: Trusted Software Development System (TSDS)

Subtask Objective: To provide an integrated set of software engineering tools which aid in improving the quality and reducing the cost of WWMCCS Standard Software and which facilitate the certification of software which processes classified information in WWMCCS ADP systems.

Subtask Description: The TSDS will be implemented on the CCTC Reston Developmental Computer system. It will be an integrated facility for analyzing, specifying, designing, implementing, testing, and managing the development of software which must be highly reliable, including security-related software which is to be certified.

Scope: The TSDS will inlucde a software engineering data base management and control system, tools which facilitate the production and quality assurance of trusted software, and processors which operate on the software modules in the data base to provide project management information and design analysis data. The facility will be useful for testing and evaluating GCOS modules, developing secure subsystems, and performig certification/verification.

Issues:

The primary issue to be resolved is the set of criteria to be utilized in selecting tools for implementation in the TSDS such that its overall objectives are supported.

A secondary issue is the specification of a standard interface through which existing or future tools can be integrated into the TSDS.

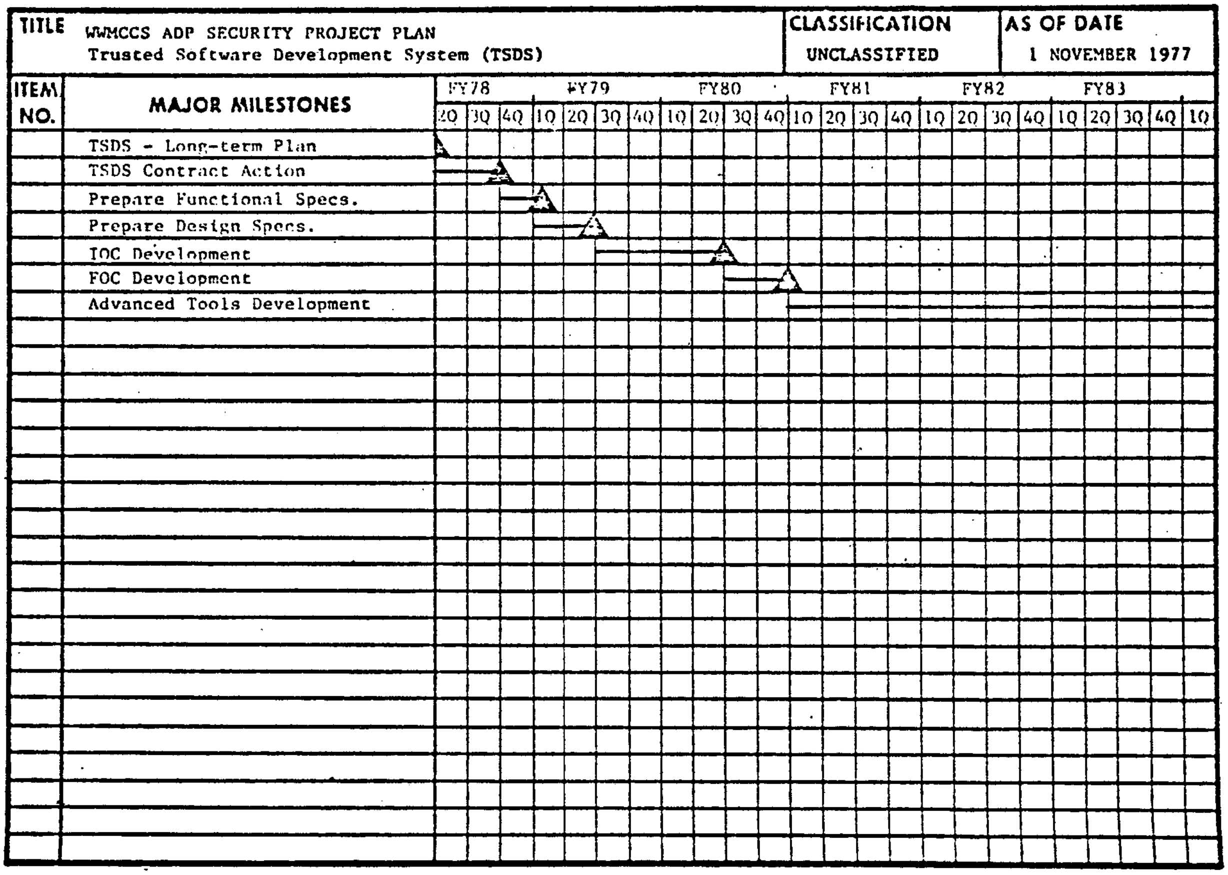
Originating Objective: 2.3.4.2 AOD:
Budget Designator: 4727302 Priority:
Subtask Title: Trusted Software Development System (TSDS)

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	6	7	6	6	6	3	34
B. RDT&E $K	267	450	250	150	150	150	1417
C. O&M $K	-	50	50	50	50	50	250
D. Procurement $K	-	-	-	-	-	-	-
TOTAL	267	500	300	200	200	200	1667

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART



Originating Objective: 2.3.4.3 AOD:
Budget Designator: 4727302 Priority:
Subtask Title: Security Software Evaluation and Maintenance System (SSEMS)

Subtask Objective: To provide, as an extension of the software engineering tools and metholologies supported by the Trusted Software Development System (TSDS), a collection of tools and techniques which support the software verification, certification and accreditation process and which aid in maintaining its credibility in an operational environment.

Subtask Description: The SSEMS will be implemented within the overall framework of the TSDS. It will provide a facility for testing, analyzing and evaluating existing software modules to ensure compliance with appropriate security criteria and aid in the overall certification process.

Scope: The SSEMS will include a collection of tools which perform such functions as flow analysis, instrumentation, verification condition generation, automated theorem proving, code comparison or other functions which aid in certifying the correctness of programs. It will interface with and operate on modules maintained in the TSDS data base.

Issues: The primary issue to be resolved is the cost/benefit aspect of formal verification given the current state-of-the-art and whether it is worthwhile to pursue formal verification. Secondary issues center around the identification of criteria against which software is to be certified and maintained and against which tools are to be selected for inclusion in the SSEMS.

Originating Objective: 2.3.4.3 AOD:
Budget Designator: 4727302 Priority:
Subtask Title: Security Software Evaluation and Maintenance System (SSEMS)

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	-	1	6	6	6	6	25
B. RDT&E $K	-	-	-	100	150	150	400
C. O&M $K	-	-	-	-	50	100	150
D. Procurement $K	-	-	-	-	-	-	-
TOTAL	-	-	-	100	200	250	550

Schedule:

Activity Unscheduled.

Originating Objective: 2.3.4.3.1 AOD:
Budget Designator: 4727303 Priority:
Subtask Title: Support for WWMCCS Accounting Program (SWAP) Certification

Subtask Objective: To technically certify to the OJCS that the SWAP extracts only those records specified and that it produces an extracted data tape that does not contain any record from the Statistical Collection File (SCF) that has classified data within it.

Subtask Description: This effort implements a plan submitted to the OJCS in response to MJCS 100-77 and J3M 1118-1977. The SWAP design will be reviewed, tests will be conducted, and controls on the program will be evaluated. The effort will be coordinated with NARDAC to ensure that user requirements are satisfied.

Scope: The effort will consist of a software security certification of SWAP, version II being developed by NARDAC.

Issues: The key issue is to determine the risk that GCOS III may inadvertantly write classified data into a designated unclassified SCF record type or into the designated unclassified SWAP extract records.

Originating Objective: 2.3.4.3.1 AOD:
Budget Designator: 4727303 Priority:
Subtask Title: Support for WWMCCS Accounting Program (SWAP) Certification

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	3	1	-	-	-	-	3
B. RDT&E $K	100	-	-	-	-	-	100
C. O&M $K	-	18	12	-	-	-	30
D. Procurement $K	-	-	-	-	-	-	-
TOTAL	100	18	12	-	-	-	130

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART

TITLE WWMCCS ADP SECURITY PROJECT PLAN SWAP Certification	CLASSIFICATION UNCLASSIFIED	AS OF DATE 1 NOVEMBER 1977

ITEM NO.	MAJOR MILESTONES	FY78			FY79				FY80				FY81				FY82				FY83				
		2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	20	3Q	40	1Q	2Q	3Q	4Q	1Q	2Q	30	4Q	1Q	2Q	3Q	4Q	1Q
	Rqmts, Threat/Risk Analysis	△																							
	Design/Implementation Review		△																						
	System Test		△																						
	System Evaluation			△																					
	OJCS Review/Approval			△																					

3.3 Security Monitoring

3.3.1 Description

Security monitoring provides ADP security officials assurance that ADP protection mechanisms are functioning and are continuously invoked. Two forms of automated assurance measures are addressed. Auditing provides a total detailed historical log of all user transactions within the system. Surveillance examines user and system activity as it occurs for the purpose of detecting potential system misuse and abuse. A centralized capability (WASSO station) will be developed for collection, analysis and reporting security related information to security officals. Strategies will be formulated and the capability extended to permit security officials to perform their duties in an intercomputer network environment.

Originating Objective: 2.3.3
Budget Designator: 4727303
Subtask Title: Prototype WASSO Station Development

AOD:
Priority:

Subtask Objective: To design, develop, install, and experiment with a prototype WASSO Station and to produce the detailed specifications for a fieldable station.

Subtask Description: A detailed four phase plan for the development of and experimentation with a prototype WASSO station has been approved by the OJCS via MJCS 263-77. Phase one, which has been completed, provided a description of the proposed functionality of the prototype station and a variety of configuration (hardware and software) alternatives. Phase two will identify issues for design experimentation, establish a test-bed station, conduct design experiments and produce a technical analysis/cost estimate for the development of a fully functional prototype WASSO station. Phase three will consist of the development of the prototype WASSO station. Phase four will consist of prototype WASSO station experimentation in an operational environment.

Scope: The prototype WASSO station will be modular and heirarchical in design such that it will be hardware and software configurable by the WWMCCS ADP sites. Hardware options will range from a terminal connected to the 65(V) front end processor, to an intelligent processing unit outboard of the host computer. The software will be modular by functions, permitting individual site configuration of WASSO station cabablities. The station will accommodate part-time to full-time manning options selectable by the local installation.

Issues: Two major issues are to be addressed:

a. Technical Feasibility

1. Soundness of this security assurance approach including hardware and software configurability

2. Impact on the operational environment (e.g., host system overhead)

3. Cost for: (a) development systems, (b) operational capabilities, and (c) maintenance

4. Evolution/growth opportunities

b. Security Utility

1. Effectiveness as a deterant to system misuse/abuse

2. Abiltiy to detect system misuse/abuse

3. Effectiveness of the WASSO/WASSO station interface

Originating Objective: 2.3.3
Budget Designator: 4727303
Subtask Title: Prototype WASSO Station Development

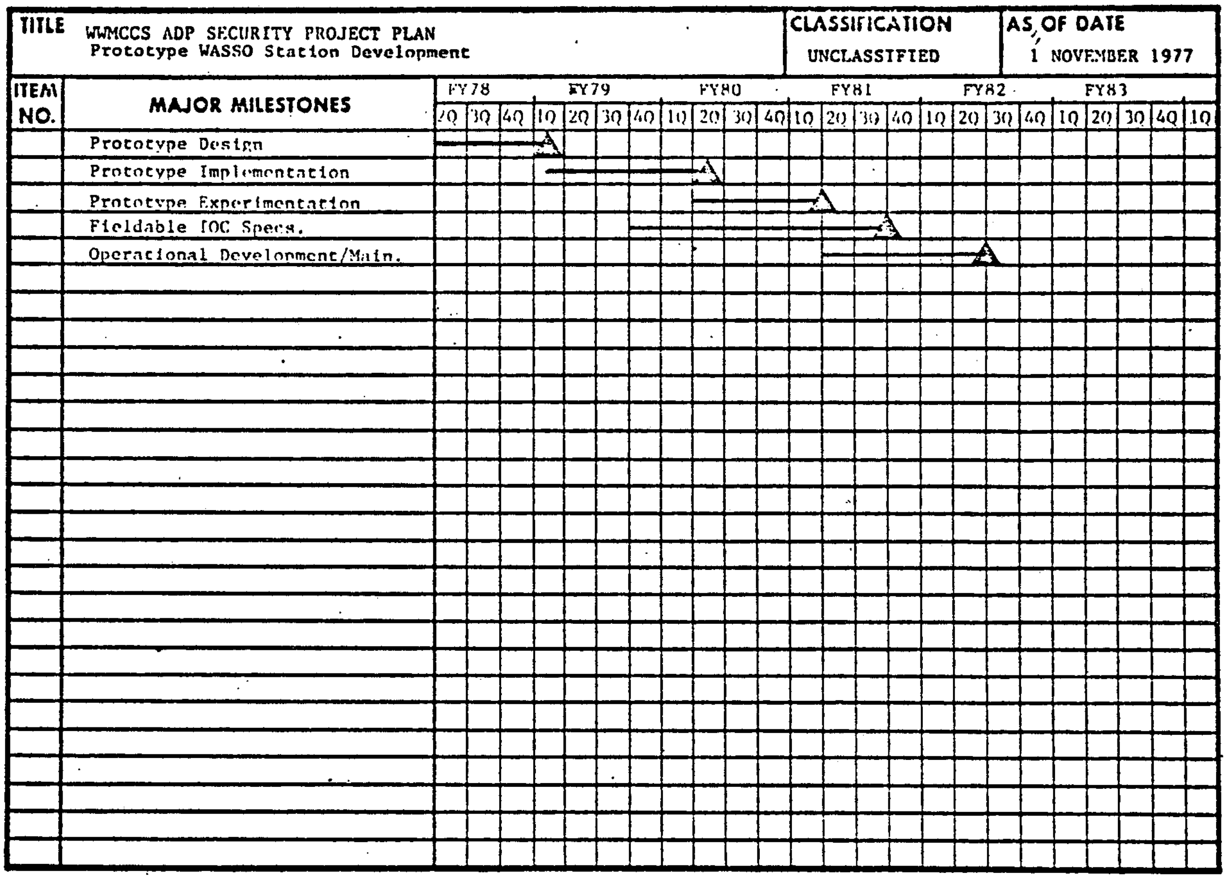
AOD:
Priority:

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	9	13	9	12	4	2	49
B. RDT&E $K	327	335	250	150	-	-	1062
C. O&M $K	-	100	169	178	74	-	521
D. Procurement $K	-	-	-	-	-	-	-
TOTAL	327	435	419	328	74	-	1583

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART


TITLE WWMCCS ADP SECURITY PROJECT PLAN
Prototype WASSO Station Development

CLASSIFICATION UNCLASSIFIED

AS OF DATE 1 NOVEMBER 1977

Originating Objective: 2.3.3.1 AOD:
Budget Designator: 1727303 Priority:
Subtask Title: Statistical Collection File (SCF) Improvements

Subtask Objective: To ensure that meaningful audit data is collected with minimal impact on the operational efficiency of the 65(V).

Subtask Description: The SCF provides a basis from which to collect meaningful security-related data as events occur within GCOS III. This is required to provide effective auditing of system operations. However, the records currently collected for this file have limited information, and no information in some cases. This subtask will address such deficiencies and implement improvements.

Scope: SCF improvements will encompass all changes to the SCF including those required for performance evaluation, operations management, etc., as well as security-related auditing.

Issues: The major issue to be addressed in this subtask is to determine the impact of internal software recording of event data on the proper execution of that event and subsequent events.

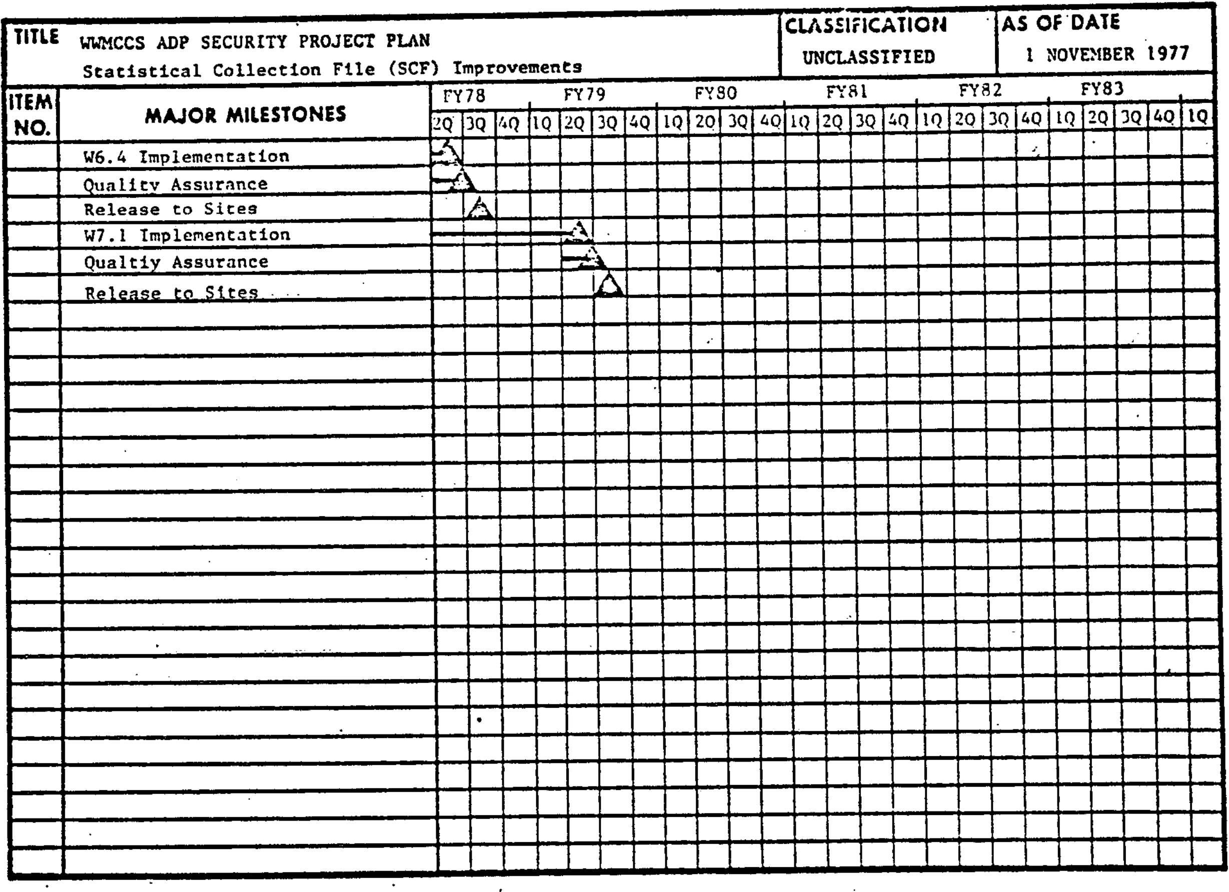
Originating Objective: 2.3.3.1 AOD:
Budget Designator: 1727303 Priority:
Subtask Title: Statistical Collection File (SCF) Improvements

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	3	1	-	-	-	-	4
B. RDT&E $K	-	-	-	-	-	-	-
C. O&M $K	55	32	-	-	-	-	87
D. Procurement	-	-	-	-	-	-	-
TOTAL	55	32	-	-	-	-	87

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART



TITLE WWMCCS ADP SECURITY PROJECT PLAN
Statistical Collection File (SCF) Improvements

CLASSIFICATION UNCLASSIFIED

AS OF DATE 1 NOVEMBER 1977

ITEM NO. MAJOR MILESTONES

W6.4 Implementation
Quality Assurance
Release to Sites
W7.1 Implementation
Qualtiy Assurance
Release to Sites

3.4 Network Security

3.4.1 Description

Network security provides external host access control to the individual host systems comprising the WWMCCS intercomputer network, and limited audit data and an interface to local assurance capabilities. The focus is on development of a secure network front-end capability which will assist in isolating users from one another and directing them to authorized subsystems. Two versions of the NFE will be produced in conjunction with Task 4727202, each supporting increased or improved network and/or security capability. Additional capabilities will be evaluated and developed to ensure only authorized access by local and network users through data base directories.

3.4.2 Subtask Interrelationships

The Network Security Task is comprised of three subtasks: (1) Network Front End (NFE) security, (2) Secure Front End Processor (SFEP) development, and (3) Secure UNIX development. The three subtasks will bring to bear an emphasis on specific research questions which must be answered in order to provide secure connectivity and interoperability for a WWMCCS computer network environment. Subtask 1 will concentrate on the overall WWMCCS/DIN II security requirements and will ultimately focus on developing a secure NFE for WWMCCS. Subtasks 2 and 3 are cooperative research efforts managed principally by DARPA. The SFEP effort (Subtask 2) will concentrate on hardware issues such as the use of descriptor-based architecture for security support, and the use of a software implemented security kernel. The Secure UNIX effort (Subtask 3) will focus chiefly on software research issues with the intent of producing a certifiability secure version of the UNIX operating system for DoD. Both Subtasks 2 and 3 will support the general development of Subtask 1, channeling the results of the SFEP and Secure UNIX efforts into context for the WWMCCS environment.

Originating Objective: 2.3.2.2 AOD:
Budget Designator: 4727304 Priority:
Subtask Title: Network Front End (NFE) Security

Subtask Objective: This subtask has multiple objectives:

a. Near-Term objectives are (1) to provide an on-going assessment of network security problems, and (2) to produce a security requirements specification for the Phase B NFE.

b. Far-Term objectives are (1) to assess and select one of the alternatives for a secure NFE, and (2) to develop the security specifications for the production version of the secure NFE.

Subtask Description: The Phase B NFE development effort will produce an interim device interfacing host computers to the AUTODIN II communications network in the January 1979 time-frame. This subtask will provide a security requirements analysis/specification for the Phase B NFE. In addition, this subtask will address the far-term objective of producing a secure NFE for WWMCCS/DIN II use. The Phase C NFE will be a hardened version of the Phase B NFE providing significantly improved and enriched security features. The Phase C NFE is currently unfunded. The Phase D NFE is the last currently planned NFE. It will be multilevel secure and will be the result of an assessment of such developments as SFEP, Secure UNIX, and BLACKER I (NSA).

Scope: The NFE will provide a wide range of operational capabilities. This subtask, however, will concentrate on developing the NFE security functionality. In addition, the NFE device itself will play a significant role in the development of a distributed subsystem architecture or nodal network.

Issues: The following set of issues will be addressed by this subtask:

a. Feasibility of a security kernel in the NFE

b. Success of the Secure UNIX, SFEP and BLACKER I efforts

c. Resolution of DIN II (but non-WWMCCS) security requirements for the NFE

d. Security requirements vs. performance characteristics trade-offs.

Originating Objective: 2.3.2.2
Budget Designator: 4727304
Subtask Title: Network Front End (NFE) Security

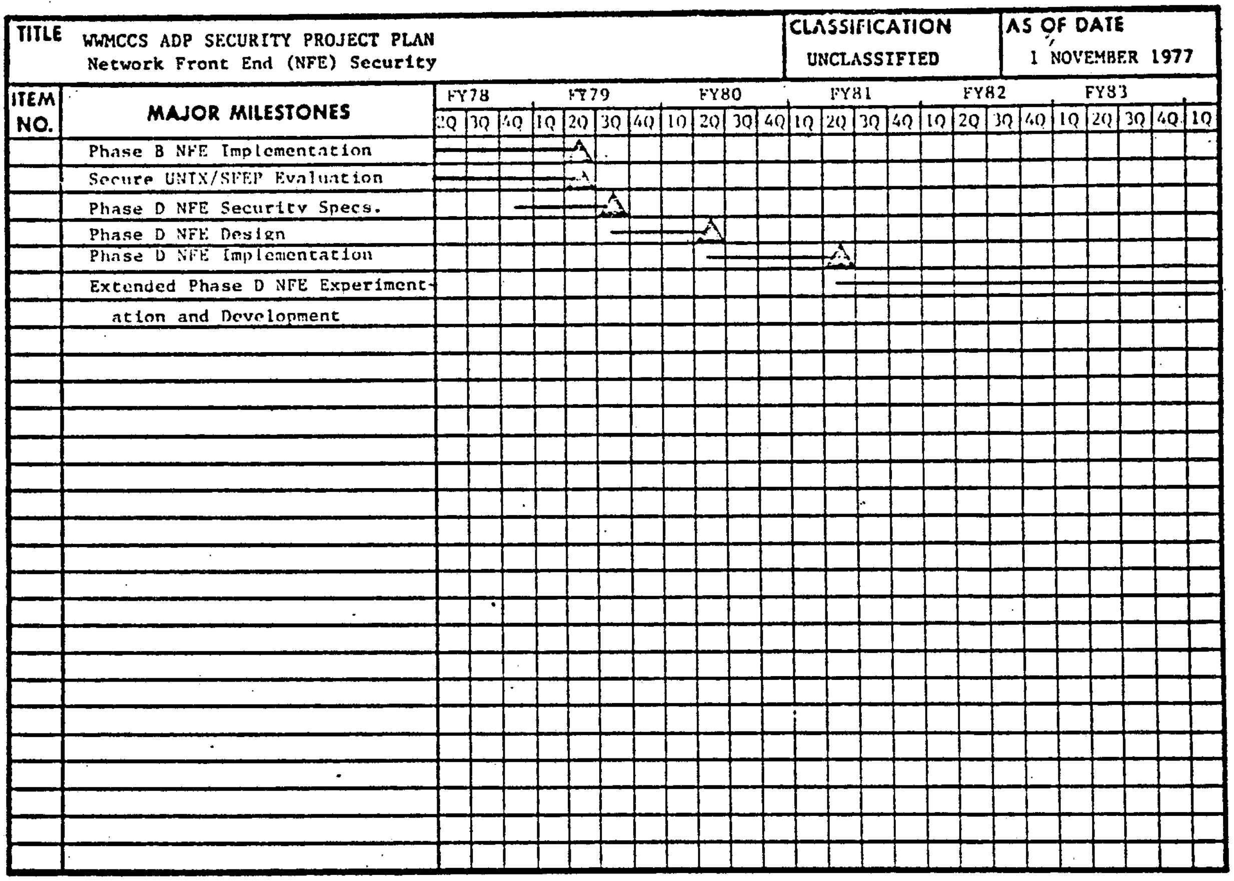
AOD:
Priority:

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	14	12	12	6	6	6	56
B. RDT&E $K	231	220	300	300	300	300	1651
C. O&M $K	-	-	-	-	-	-	-
D.Procurement $K	-	-	-	-	-	-	-
TOTAL	231	220	300	300	300	300	1651

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART



TITLE WWMCCS ADP SECURITY PROJECT PLAN
Network Front End (NFE) Security

CLASSIFICATION UNCLASSIFIED

AS OF DATE 1 NOVEMBER 1977

Originating Objective: 2.3.2.2 AOD:
Budget Designator: 4727304 Priority:
Subtask Title: Secure Front End Processor (SFEP) Development

Subtask Objective: To support the development of a production prototype secure front end processor applicable to a wide variety of secure applications, including evaluation as an alternative for the standard NFE for the WWMCCS Intercomputer Network, and as a secure terminal concentrator for the Experimental WWMCCS Nodal Network (EWNN).

Subtask Description: The SFEP is a secure minicomputer-based front end communications processor suitable for connection of hosts to AUTODIN II and/or EWNN. The project is under the joint sponsorship of DARPA, CCTC, and NSA, with DARPA providing overall project management. The security approach is based on using a commercial Honeywell Level 6/40 minicomputer augmented by a security protection module yeilding an architecture similar to that of Multics, and suitable for security kernel implementation.

Scope: The SFEP subtask will provide the design, development, test and evaluation, and verification of a production prototype version of the secure Level 6/40 minicomputer as well as a network interface controller for connecting it to a packet-switched network. In addition, a security kernel based on the Secure UNIX operating system will be designed for the SFEP.

Issues: The primary issue to be resolved is the suitability of UNIX, which is a PDP-11 operating system, for implementation on the SFEP. Secondary issues include the resolution of a page-fault recovery problem in the security protection module, and whether the network interface controller can be used for a variety of networks.

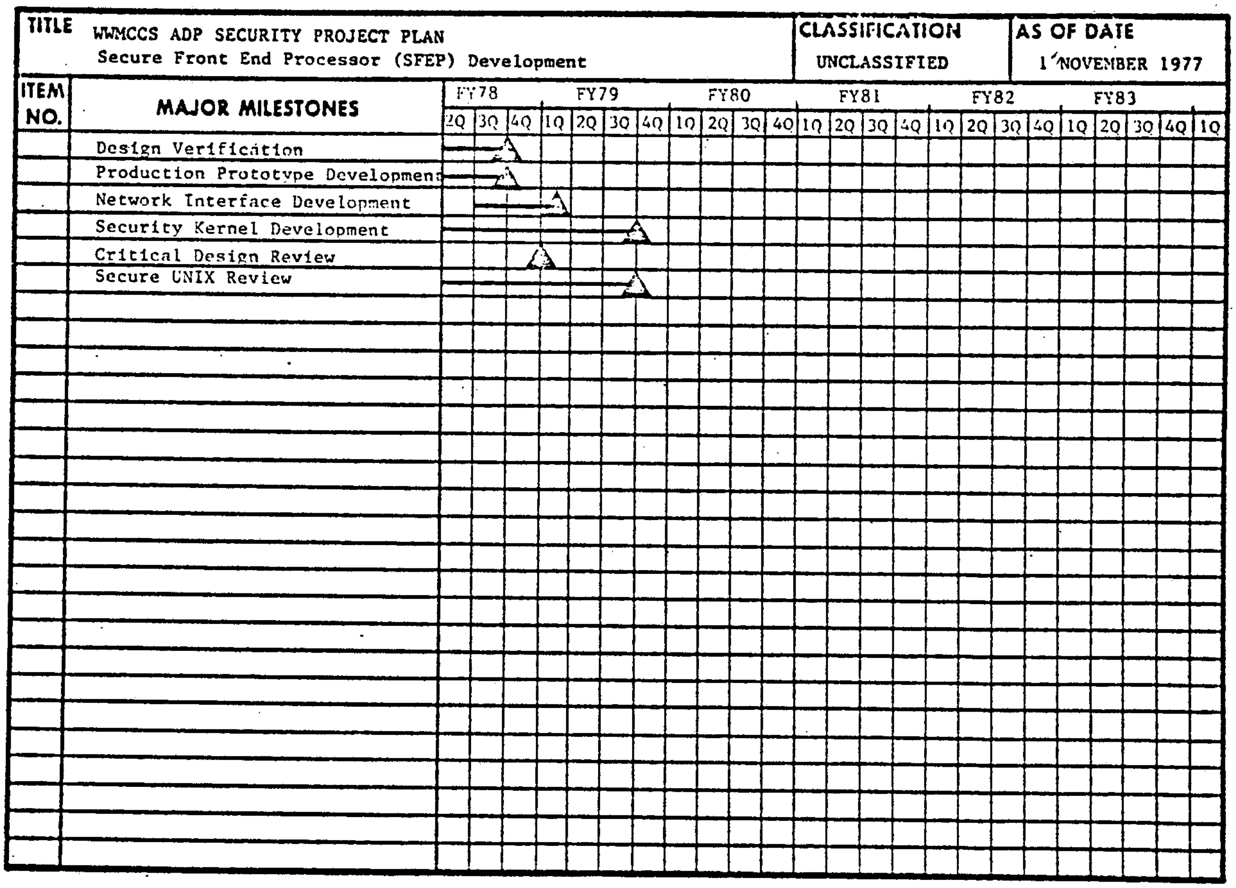
Originating Objective: 2.3.2.2 AOD:
Budget Designator: 4727304 Priority:
Subtask Title: Secure Front End Processor (SFEP) Development

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	1	1	-	-	-	-	2
B. RDT&E $K	150	100	-	-	-	-	250
C. O&M $K	-	-	-	-	-	-	-
D. Procurement $K	-	-	-	-	-	-	-
TOTAL	150	100	-	-	-	-	250

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART


TITLE WWMCCS ADP SECURITY PROJECT PLAN
Secure Front End Processor (SFEP) Development

CLASSIFICATION UNCLASSIFIED

AS OF DATE 1 NOVEMBER 1977

Originating Objective: 2.3.2.2
Budget Designator: 4727304
Subtask Title: Secure UNIX Development

AOD:
Priority:

Subtask Objective: To build into the existing UNIX operating system a security kernel which can be certified, while having minimum impact on performance. To provide a secure minicomputer operating system applicable to a wide range of applications.

Subtask Description: The purpose of this effort is to design, implement, document and verify a production quality, certifiably secure version of the UNIX operating system for the PDP-11 computer. A potential application for the operating system is the WWMCCS/DIN II NFE. This effort is jointly sponsored by DCA, DARPA and NSA with DARPA providing overall project management.

Scope: The secure UNIX operating system is to be initially implemented on a PDP-11/70. It will also be implemented on a Honeywell Level 6/40 with the security protection module being developed under the SFEP effort.

Issues: The principal issues are (1) whether or not the UNIX operating system can be successfully retrofitted with a security kernel implementing the Bell and LaPadula model of security, (2) whether or not the operating system interfaces can be properly retrofitted, and (3) what imact these changes will have on system performance.

Originating Objective: 2.3.2.2
Budget Designator: 4727304
Subtask Title: Secure UNIX Development

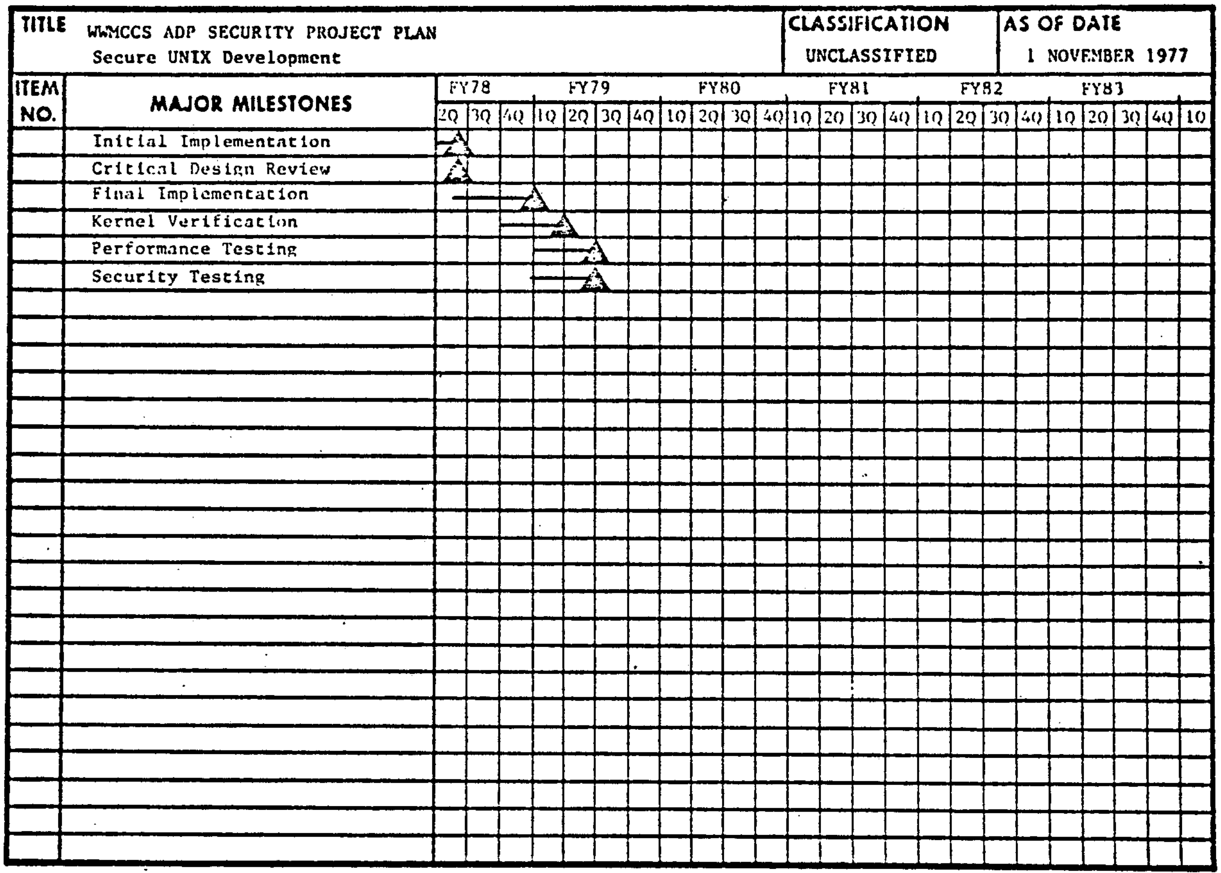
AOD:
Priority:

Resources:

	FY78	FY79	FY80	FY81	FY82	FY83	TOTAL
A. In-house M/M	1	1	-	-	-	-	2
B. RDT&E $K	55	55	-	-	-	-	110
C. O&M $K	-	-	-	-	-	-	-
D. Procurement $K	-	-	-	-	-	-	-
TOTAL	55	55	-	-	-	-	110

Schedule:

DEFENSE COMMUNICATIONS AGENCY MILESTONE CHART



APPENDICES

PROGRAM OBJECTIVES AND ORIGINAL TASKING

SUMMARY

A. WWMCCS Policy and Program Objectives

Department of Defense security policy is defined in DoD 5200.1-R, "Information Security Program Regulations". It is the basic policy document dealing with the protection of defense information. It requires that National Security Information be protected against unauthorized disclosure, and identifies how and by whom information may be classified.

DoD ADP security policy is derived from DoD 5200.1-R and is provided in two complementary documents: DoD 5200.28 and DoD 5200.28-M. DoD 5200.28 provides guidance as to how ADP system security should be applied. It is from the minimum requirements listed in this policy that WWMCCS ADP security requirements and objectives are derived. These security requirements include:

"o individual accountability

o environmental control

o system stability

o data integrity

o system reliability

o secure communications links

o protection of classified material. "(1)

DoD 5200.28-M, "Manual of Techniques and Procedures for Implementing, Deactivation, Testing and Evaluation of Secure Resource Sharing ADP Systems" specifies acceptable techniques for implemention of the security requirements required in DoD 5200.28. Neither DoD 5200.28 nor DoD 5200.28-M provides sufficient technical guidance for the security enhancement or development of ADP systems to provide multilevel ADP security.

(1) DoD 5200.28, Security Requirements for Automatic Data Processing Systems, 18 Dec 72.

The basic WWMCCS ADP security objective has been expressed in terms of capabilities for sharing various types of system resources among various types of users. JCS PUB 19 identifies a number of objectives which specifically address ADP security and other objectives on which security will have an impact. A summary of these objectives includes:

"CM-200. Continuity of Operations. Provide for continuity of ADP operations through an integrated WWMCCS ADP system, secure as required, using distributed data base concepts, intercomputer network capabilities, workload sharing techniques that will support continuity of ADP operations throughout the spectrum of operations.

(a) Provide automatic switching of data through a multiplicity of modes/nodes so that the system will be less vulnerable to enemy actions.

(b) Provide secure data interfaces with designated ADP systems that support the WWMCCS to achieve the objective of an interactive and mutually supportive command and control system.

(c) Provide procedures and files structured to use the distributed data base concept to the optimum extent while insuring the accessibility of those critical portions of the data base required for survivability and responsiveness by duplication at multiple locations.

CM-202. System Software. Provide the WWMCCS ADP system with a multilevel secure standard operating system which supports time-shared, near real time, interactive, and distributed data base capabilities.

CM-204. ADP Security. Provide a capability to exchange data between and within automated systems with appropriate security/privacy safeguards against compromise of data within the ADP systems accessed.

(a) Provide mulitlevel security safeguards for resource-shared ADP systems with remote terminals having varying degrees of security protection.

(b) Provide TEMPEST certified remote peripherals and network processors.

(c) Provide system wide protection against accidental or deliberate intrusion which would tend to deceive the user or compromise data acquisition, transmission, storage, proccessing or dissemination.

(d) Provide for the isolation of the WWMCCS ADP system from its potentially hostile environment to insure that only authorized users obtain appropriate access to the system.

CM-205. Information Display. Improve the capability for displaying all types of information required for command and control.

(c) Provide an appropriately protected, integrated, real time means of displaying the security classification (and special access information, if appropriate) of the data on the information display.

M-206. Hardware. Provide the:

(a) Support of secure ADP system interactions within and between designated WWMCCS facilities.

(b) Modification or replacement of WWMCCS ADP systems with appropriate consideration of configuration management.

CM-207. Intelligence Support. Provide for secure data exchange between designated intelligence and WWMCCS computers."(1)

SM-283-72 expands on these objectives. The target developmental objective remains the capability to operate in a multilevel secure mode.

Accordingly, system security is key in the first and second of three development phases:

Phase I Objective (FY72-74). "Development of detailed security measures and procedures within the WWMCCS. These measures and procedures will include those pertaining to hardware, software, facilities, personnel, and communications."

Phase II Objective (FY75-78). "Implementation of a WWMCCS ADP Program which has the capability to exchange data between automated systems must include appropriate security/privacy safeguards against compromise of the information being handled. Each WWMCCS user is dependent upon this capability for storage, retrieval and exchange of classified information. Safeguards must be incorporated into online, resource-shared ADP systems with remote terminals having varied degrees of security protection. The capability for remote querying of classified data bases and transmitting

[1] JCS Pub 19, WWMCCS Objectives and Management Plan, Vol. III, Annex A, Apr 77.

classified information over common-user digital links is also required."(1)

B. WWMCCS ADP Program Tasking

The OJCS formed specific security program guidance and direction for DCA/CCTC/WWMCCS ADP Directorate (WAD). A refinement of WWMCCS security objectives and tasks is identified in several documents. The first guidance paper is SM-593-71. This paper identifies three distinct areas in which the WAD Security Program is to concentrate its RDT&E resources:

"a. Development of Improved Multilevel Security Techniques and Analysis of Security Features.

(2)(a) A security feature analysis of the WWMCCS New Standard System will be required to determine if new capabilities or enhancements are required to provide multilevel security protection.

(2)(b) Safeguard requirements must be analyzed for remote terminals located in areas of varying degrees of security protection and for exchanging various security levels of information between WWMCCS sites which may vary in their site security classification.

(2)(c) Security analysis must be performed to assure necessary capability to safeguard the physical and logical separation of site unique data from WWMCCS common (system) data regardless of level of security classification.

(2)(d) Safeguard features must be provided for:

1. Access identification

2. Access accountability

3. Site Security

4. Hardware and communications protection

5. Software protection

6. File maintenance security

7. System security

(1) SM-283-72, WWMCCS ADP Program: Mid-Range Plan, 10 Jun 72.

8. Personnel security.

(2)(e) Capabilities to improve the security protection afforded to the users of the system in a resource shared environment, especially for the online, remote access type of operation, should be developed.

b. Major Upgrade of WWMCCS New Standard Data Management System (DMS) Modules.

(2) It is expected that major improvements to the WWMCCS New Standard DMS will be required to achieve the target DMS capable of operating in the target WWMCCS ADP System under a concept of distributed data bases in an intercomputer network, with remote online and multilevel security features.

f. Development of ADP Network Features.

(2)(g) Development of configuration design criteria for security (hardware/software security features) both within and between WWMCCS ADP system which must comply with DoD Directive 5200.28 and DCID 1/16."(1)

The second WWMCCS ADP security guidance paper is SM-150-73. The purpose of this document is to implement DoD 5200.28 and DoD 5200.28-M for WWMCCS ADP. The guidance states that in concept:

"a. ADP system security will be achieved by utilizing a combination of conventional security procedures and new automated techniques which will include the following:

(1) ADP hardware features.

(2) ADP software features.

(3) Communications security.

(4) Emanations security.

(5) Physical security measures.

(6) Personnel security measures.

(7) Procedural safeguards (management, administrative, and operational procedures).

(1) SM-593-71, RDT&E Program in Support of the WWMCCS Standard System, 7 Sep 71.

b. Man will remain the most important link in the security chain.

c. An evolutionary approach will be taken in developing and implementing system security measures."(1)

The WAD Security Program responds specifically to the following SM-150-73 tasking:

"(1) Recommend to the Joint Chiefs of Staff the most technically feasible and cost-effective ADP capabilities for multilevel security within and between systems.

(2) Prepare specifications for software and hardware security features, as required.

(3) Develop and recommend to the Joint Chiefs of Staff standards for ADP security hardware and software features and procedural safeguards. This will include, but not be limited to, a standard user access and authentication schemes and security monitoring and auditing standards.

(4) Provide to the Joint Chiefs of Staff in the evaluation of ADP system change proposals.

(5) Develop technically feasible and cost-effective ADP security test criteria, methods, and procedures. Provide Commands, Services, and Agencies responsible for WWMCCS New Standard Systems with tests to assist in validating system security operational capabilities.

(6) Develop, analyze, test, evaluate, and recommend approval of WWMCCS ADP multilevel security standard software. Distribute and maintain standard multilevel security software which has been approved by the Joint Chiefs of Staff.

(7) Conduct security tests and evaluation with Service and Agency support, as appropriate, which will include:

(a) Validation of hardware and software security features.

(b) ADP hardware and software test and evaluation support for WWMCCS New Standard System installations.

(c) All aspects of test and evaluation to support approval of the system used within the NMCS and each WWMCCS network that involves two or more unified and specified commands, Services, or Agencies. Test and evaluation results will be furnished

(1) SM-150-73, Security Guidance for the WWMCCS ADP Systems, 27 Mar 77.

authorities having jurisdiction over the particular system or subsystem.

(8) Develop, install, analyze, test, and evaluate prototype ADP security protection system(s) in conjunction with the appropriate Services, the unified and specified commands, and/or Defense agencies.

(9) Appoint an ADP System Security Officer(s) for the Prototype WWMCCS Intercomputer Network (PWIN). Based on PWIN experience, make recommendations to the Joint Chiefs of Staff regarding the accomplishment of this function for the operational intercomputer network."(1)

The third WWMCCS ADP security guidance paper is SM-446-75, Establishment and Support of WWMCCS ADP Security Functions, 8 AUG 75. The guidance tasked the WWMCCS ADP Directorate to plan, program, budget for, develop, install and operate a prototype WASSO station as approved by the WWMCCS ADP Project Manager, as a matter of priority. A plan was prepared and conditionally approved by the OJCS for this development on 9 MAR 75 (SM-477-75). Upon completion of the first of six phases a recommendation of candidate automated WASSO functions and a configurable hardware and software prototype architecture were presented to the OJCS, and an updated project plan was submitted 8 April 1977. OJCS approved the results of Phase I and authorized continuancee of the project to Phase III of the revised four phase plan (MJCS-263-77) on 31 AUG 77. A Technical Analysis/Cost Estimate for the prototype WASSO station will be submitted to OJCS for approved prior to proceeding with Phase III (Implementation Phase) as directed.

(1) SM-150-73,Security Guidance for the WWMCCS ADP Systems, 27 Mar 73.

MULTI-LEVEL SECURITY TECHNICAL ANALYSIS/COST ESTIMATE

SUMMARY

A. Background

In March 1976 DCA/CCTC produced a Technical Analysis/Cost Estimate (TA/CE) for the purpose of providing WWMCCS Management with information on which to evaluate the possible alternatives which are considered feasible for providing a multi-level secure system base for WWMCCS ADP. A course of action was recommended based on conclusions reached following a comparative analysis of the following system hardware bases:

- o Honeywell Series 6000
- o Honeywell Series 60 (Level 66)
- o Honeywell Series 60 (Level 68)
- o Non-Honeywell Systems

Steps taken in developing the TA/CE included:

(1) Identification of alternatives;

(2) Development of technical feasibility factors;

(3) Collection of data and comparative analysis of alternatives.

The following technical feasibility factors were developed to serve as the set of criteria to be used in assessing the system base alternatives and performing a comparative analysis:

(1) Security

(2) Cost/benefit

(3) Life cycle

(4) WWMCCS performance

(5) WWMCCS functionality

(6) Reliability

B. Comparative Analysis

Alternative A - Honeywell Series 6000/GCOS III

Major advantages:

- o Maximum utilization can be made of existing hardware.
- o Will support secure software-based subsystems.
- o Can serve as processing node in secure distributed system architecture.
- o Costs to develop security enhancement options low relative to total investment or costs of other alternatives.
- o Peformance predictable, measurable and readily evaluated. Improvements likely to be successful.
- o Resources invested in networking protected.

Major disadvantages:

- o System is not secure.
- o Major redesign required to make system secure.
- o Level of protection outside secure subsystems would remain low.

Alternative B - Honeywell Level 66/GCOS 66

Major advantages:

- o Will likely provide necessary structures for MLS system.
- o Will support secure software-based subsystems.
- o Can serve as processing node in secure distributed system architecture.
- o Costs of conversion and user retraining minimal as compared to Alternatives C and D because of GCOS III compatibility objective.
- o Should provide increased WWMCCS functionality with emphasis on interactive applications and enhanced data management facilities.

Major disadvantages:

o Securiity is an overall system development objective, but specific security objectives not identified.

o Actual level of protection is not known.

o Improvements to security design of GCOS 66 would require DoD funding at extremely high cost, probably in excess of $20M over 3-5 years.

o Capital outlay for hardware could reach $50M for all twenty-nine sites.

o GCOS 66 security features not available for another 2.5 years.

Alternative C - Honeywell Level 68/MULTICS

Major advantages:

o Provides the necessary structures for MLS system.

o System designed with security as an objective.

o Can serve as processing node in secure distributed system architecture.

o Should provide performance improvement over present system for interactive applications.

Major disadvantages:

o Current MULTICS system is not multi-level secure.

o Capital outlay for hardware could reach $100M for all twenty-nine WWMCCS sites.

o Level of effort and costs of application conversion to MULTICS would be exceedingly high.

o Would not support WWMCCS data management systems.

o The life expectancy of MULTICS as a standard product is uncertain in the future.

o Extensive user retraining required due to different user interface.

Alternative D - Non-Honeywell Systems

Major advantages:

o Could probably support secure software-based subsystems.

o Could probably serve as processing node in distributed system architecture.

o Systems exist which could outperform the present system and which are more reliable.

Major disadvantages:

o No large-scale commercially available system exists which provides an acceptable level of security.

o Hardware procurement costs would far exceed that of other alternatives.

o Conversion costs would probably be at least twice that of MULTICS.

o Complete re-orientation of computer support personnel would be reqiuired.

C. Recommended Course of Action

Computer technology is now evolving toward increased decentralization of processing from large general purpose computers into networks of smaller computers. Made economically feasible by the availability of microprocessors at mass production prices, this new focus now allows systems to be built which can be tailored to meet specific processing requirements and easily modified to meet future needs.

WWMCCS ADP is now evolving toward networking, large shared data bases and standard user interfaces. Yet most processing is still done in a serial fashion with costly time delays and little of the real-time capability which is essential in the command and control environment. Efforts to improve security, such as split systems and periods processing, are clearly incompatible with the evolutionary direction cited and future goals for WWMCCS ADP. The costs and risk of clearing increasing numbers of users under the system high concept will increase as the system evolves.

In consideration of these factors the following actions were recommended to the WWMCCS ADP PMO:

(1) RETAIN HONEYWELL SERIES 6000/GCOS III SYSTEM BASE

The retention of this system involves the lowest level of risk and smallest cost increment of those considered. It permits a deliberate and phased transition from monolithic systems to distributed systems with minimum disruption and the gradual introduction of new functional subsystems which satisfy WWMCCS security requirements.

(2) ENHANCE GCOS III SECURITY

In lieu of a MLS O/S, continue to assess the security weaknesses of GCOS III and develop SDN's for improving the system security. Improved techniques should continue to be sought for user authentication, automated physical access control, security monitoring and other areas which are peripheral to the main protection capabilities of the operating system.

(3) DEVELOP SECURE GCOS-RESIDENT SUBSYSTEMS

To provide an improvement in the level of protection of GCOS III, the development of secure GCOS-resident subsystems should be further pursued. In particular the Secure Transaction Processing Subsystem, which is under development and which functionally replaces several transaction processing systems in WWMCCS, should be completed.

(4) DIRECT SYSTEM ENGINEERING TOWARD DISTRIBUTED SYSTEMS

This approach would merge the planned evolution of WWMCCS with predicted trends in computer technology while providing the most cost-effective solution to the security problem. The likelihood of producing certifiably secure software (or firmware) for microprocessors with limited functionality and well-defined interfaces is much greater than that of developing secure operating systems for complex third generation computers.

(5) DEVELOP DATA BASE MACHINE & DISTRIBUTED DATA BASES

The security implications of data base machines and distributed data base technology should be fully investigated and applied to the production of secure distributed subsystems for WWMCCS. Current research and development of a data base machine should continue and the results applied toward the production of a data base machine as a functional subsystem in the prototype local distributed processing network.

(6) DEVELOP SECURE MICROPROCESSOR BASED SUBSYSTEMS

The security aspects of microprocessor-based subsystems, utilized both as processing nodes in a distributed system architecture and as user interfaces in hybrid functional terminals should be fully investigated and the results applied as a tool in testing and evaluating the security characteristics of microprocessor-based functional subsystems and in developing prototype subsystems for application in the initial local distributed processing network.

(7) DEVELOP LOCAL SECURE DISTRIBUTED PROCESSING NETWORKS

With a secure distributed system architecture as a long-term goal for WWMCCS ADP, a prototype secure distributed processing network should be developed at a selected WWMCCS site. The present Series 6000 system would serve as its nucleus and the necessary security improvement would be reached by isolating sensitive processing functions into secure distributed subsystems.

SECURITY PROGRAM HISTORY

A. WWMCCS Automatic Data Processing

The WWMCCS Objectives Plan and the WWMCCS Mid-Range Plan emphasized the need for improved, coordinated command and control functions and facilities, especially to provide the National Command Authority (NCA) comprehensive, accurate and timely information regarding options and capabilities for plans and operations. It was expected that automatic data processing would constitute an important resource in the fulfillment of this need, as indicated by the following programs:

o A standard ADP hardware procurement program

o Programs to consolidate and share the data processing resources by converting the command-and-control applications to the WWMCCS New Standard ADP System at the WWMCCS data processing installations.

o A program to provide effective and efficient management of the WWMCCS Standard ADP System through the centralization and augmentation of system planning, organization and control funtions in the Joint Staff (J-32).

o The Joint Technical Support Activity (JTSA) - to provide central technical support to the WWMCCS community for ADP developments. Such programs include the Prototype WWMCCS Intercomputer Network (PWIN), the World-wide Data Management System (WWDMS), WWMCCS ADP Computer Performance Evaluation and Maintenance, and WWMCCS ADP System Security.

B. WWMCCS ADP System Security

At the same time, the security of WWMCCS ADP systems was either considered in the conventional perspective of physical, personnel and communications security, or it was considered in the perspective of GCOS augmentations being developed by Honeywell Information Systems, Inc. in response to the procurement specifications. The situation was characterized by the following conditions:

o There was a lack of generally understood and accepted security definitions and standards, especially as they pertained to vulnerabilities, security acceptance criteria, and technologies of computer security design and implementation.

o There was a diversity of computer security needs, both real and percieved, but there was little appreciation of their nature or extent. Computer security was considered as an implicit quality to be delivered by the vendor.

o Computer security had been inadequately included as a design parameter in nearly all commercially developed ADP systems, including the H6000 Series. Moreover, there was little agreement on how to cope with such deficiencies.

o The computer-security state-of-the-art did not offer solutions either to the problem of providing secure resouce sharing computers or to the problem of assessing computer security adequacy. The only technically feasible approach for securing the WWMCCS ADP system was monolithic operations (i.e., dedicating the system to one security classification and clearance level). Such an alternative was not acceptable in light of WWMCCS operational needs.

The JTSA contracted with the System Development Corporation (SDC) in early 1973 for WWMCCS ADP security analysis studies. SDC was charged with answering the following questions:

1. What are the WWMCCS.ADP security requirements?

2. What are the technical capabilities and limitations of WWMCCS ADP with respect to computer security?

3. What security modes are feasible for operating WWMCCS computers in the 1973-1978 timeframe (i.e., the existing systems)?

4. What security modes are feasible for operating WWMCCS computers after 1978 (i.e., the target system)?

5. What are the computer security principles applicable to the evolution or procurement of future WWMCCS computer systems?

C. The Basic Contract Scope

The project consisted of three phases of research in WWMCCS ADP security. The first phase was devoted to an analysis of the WWMCCS ADP environment to ascertain the operational requirements for security in WWMCCS ADP and to determine the conceptual issues which underlie a security assessment of the current system and any possible enhancement recommendations. The second phase was devoted to a security investigation and assessment of the current WWMCCS technical base, including the WWMCCS New Standard Computer System hardware and software, the emerging resources for WWMCCS networking (particularly the PWIN), and the user-system interface. The third phase was devoted to the formulation and recommendation of WWMCCS ADP security principles, alternative WWMCCS ADP security feature design and implementation.

In general the Basic Contract established a conceptual baseline for coping with WWMCCS ADP security problems and recommended a research and development program for producing useful computer security enhancements.

The following are the major specific products of that effort:

o Operational Requirements for Security

Addressed the question, "What does the WWMCCS ADP community require of ADP security in order to perform its missions and functions?". The major conclusion was that there is a high priority need for controlled sharing of a heterogeneous set of data and physical resources among a variety of authorized users of the WWMCCS ADP System. The community could not operate adequately in a dedicated, monolithic security mode.

o Framework for Computer Security

A document which examines an interrelated set of axioms and principles of computer security. This document has been applied in the following areas:

a. Analyzing the security of existing computer systems

b. Specifying security criteria for designing future computer systems

c. Analyzing and refining security policy

d. Performing computer security research and development.

o GCOS III Security Analysis

This analytical effort resulted in the conclusions that:

a. The WWMCCS GCOS III could not protect against penetration and abuse, and

b. The WWMCCS GCOS III could not be repaired to provide adequate control of resource sharing without major redesign and implementation.

o WWMCCS User-System Interface Security Analysis

This document describes the user-system environment, recommends a range of security personnel responsibilities, and assesses the need for fundamental and supplemental procedural controls.

- Network Security Analysis

  The studies were conducted to analyze the security implications of WWMCCS Computer Networking and to recommend possible approaches. It surfaced the need and applicable approach in WWMCCS of providing security in a computer network through the use of intelligent cryptographic devices and a central security controller.

- WWMCCS ADP Security Development Program

  This document constituted the final report of the Basic Contract, and it recommended a comprehensive centralized technical program in three phases for achieving controlled sharing in a closed environment by the end of FY78. This program was presented to the WWMCCS Council Support Group.

The program defined in the above reference consisted of three phases roughly equivalent to the security modes described in security policy:

- Phase I- Dedicated mode providing physical separation or isolation of different types of classified information and users either during different periods of the operational day or on separate computers, or both.

- Phase II- Compartmented mode providing the separation or isolation of different types of classified information and differently cleared users on the same hardware configuration.

- Phase III- Full-Sharing mode establishing fully controlled sharing of data and physical resources among individual users according to their individual access needs and approvals.

Figure 1.1 illustrates the Program flow that was recommended. Starting with isolated operations, a path can be traced to any work area in the Program to permit both maximum parallelism in pursuing program objectives and emphasis on work areas with expected high pay-off. As the Program proceeded, the Program flow proved its versatility.

The programmatic focus at this time was to make the greatest quantum jump in security capability possible, i.e., to get the biggest bang for the buck. Consequently, when Honeywell offered the Level 66 New System Architecture as a system alternative, primary attention was devoted to the consideration of this offer as opposed to other elements of the recommended program.

D. The First Major Contract Increment

Earlier expectations of achieving multilevel security by 1978 were being reassessed and a program to enhance WWMCCS ADP security was given higher priority. The scope of work was expanded for SDC in the first major contract extension.

In general the scope of the contract extension was defined according to the following major types of technical support:

1. Security Requirements Analysis
   a. Operational Requirements
   b. Technical Requirements
2. Security Analysis of WWMCCS ADP
   a. System Hardware and Software
   b. Networking and Communications
   c. User-System Interface
3. Security Enhancement Program Planning
   a. Objectives and Strategies
   b. Program Elements
   c. Resource and Schedule Requirements
4. Research and Development Support
   a. Basic System Enhancement
   b. Network Security Development
   c. Functional Security Development

The bulk of the effort was directed at exploring ways of compensating for the security deficiencies of GCOS III; upgrading to Level 66; encapsulating untrusted users in secure subsystems; and encapsulating separate copies of GCOS III in virtual machine environments. The problem was that all approaches were technically feasible if other factors (e.g., the hardware; costs; performance allowances) could be adjusted to suit the approach, and this was a proposition of dubious general acceptability. Moreover, much of the potential of each approach was directly related to Honeywell's intentions and capabilities, and these were never clearly and fully committed.

Specific accomplishments were achieved in the following areas:

- Level 66 New System Architecture Analysis

    A team of government and SDC personnel conducted a preliminary assessment of Honeywell security objectives and plans for the Level 66 New System Architecture. The major conclusions were that the hardware architecture could provide an adequate base for controlled sharing, but that not enough was known about the GCOS 66 (then GCOS IV) operating system to recommend a WWMCCS committment for acquiring the system. It was recommended that a cooperative effort between Honeywell and the WWMCCS community be undertaken to develop further the securtiy concepts and approaches that would enable the system to be demonstrated in a clear and convincing manner that it met WWMCCS ADP security requirements. The expected cost of such an effort turned-out to be prohibitive.

- Virtual Machine Architecture Analysis

    In a major effort to explore the virtual machine approach to encapsulating GCOS III, SDC performed and documented the following studies:

    a. A Virtual Machine Monitor (VMM) Concept Analysis

    b. A VMM Feasibility Analysis

    c. A VMM Verification Criteria and Methodology Study

    d. A VMM Engineering Design.

    In addition, SDC participated in a Honeywell study of the feasibility of transferring the VMM approach used in the H6180/VMM to the Level 66 hardware environment. All such efforts were terminated at the completion of the Honeywell study when it appeared that a virtual machine environment would severely degrade performance beyond an acceptable level.

- Secure Subsystems Analysis

    This study analyzed selected WWMCCS ADP subsystems, identified major problems and issues, and recommended a plan for the development of WWMCCS ADP secure subsystems. While secure subsystems were concluded to be generally feasible, it was also concluded that no specific technical approach would be recommended without developing and experimenting with a prototype. The results also indicated that the outcome of such a "fly before buy" approach would depend not only on security factors, but also on such factors as required functionality, degree of site uniqueness, and the GCOS interfaces.

o Security Monitoring Analysis

In recognition of the need to support the WWMCCS ADP System Security Officer (WASSO) with computer supported capabilities, SDC was tasked to analyze and recommend approaches to security monitoring. This work serves as the foundation for enhancing the near-term capabilities of the WASSO and for establishing an experimental prototype WASSO station for developing target capabilities.

o Security Requirements

The Framework for Computer Security was revised to incorporate recent technical developments and to clarify a number of complex operational issues. A section was added on the subject of coping with security problems, and it focused primarily on the issues of risk analysis, guidelines, standards and measures.

o Network Security Analysis and Development

A considerable effort was made to explore and recommend several avenues to the problem of securing a WWMCCS computer network. Several recommendations were made regarding security developments of the Network Front End (NFE), the PWIN, and the overall WWMCCS Computer Network.

E. The Second Major Increment

In late 1975 the Security Program continued to grow in breadth and depth, but the highest priority issue remained the WWMCCS hardware upgrade. It was obvious that the framing of a concrete WWMCCS ADP security enhancement program depended on the resolution of this issue. Thus, while SDC was asked to proceed in the same general directions, the first order of business was to recommend what to do about the H6000/GCOS III. Consequently, a major effort proceeded to evaluate the most viable alternatives to the current system. The results were documented in a technical analysis and cost estimate (TA/CE) titled Multi-level Secure ADP Systems for WWMCCS.

Requirements Paper

Contract Inventory Document System

For

Directorate of Science and Technology

11 November 1977

TABLE OF CONTENTS

ATTACHMENTS

I. INTRODUCTION

This paper defines the requirement for a computer supported file maintenance and retrieval system which will keep track of collateral classified and compartmented material sent by the Directorate of Science and Technology to industrial and government contractors. The system is requested by the Directorate of Science and Technology as a modification to AD Study 30717BH. The modification is dated 14 September 1977.

The requirements presented in this paper are the joint
STAT effort of [redacted] Assistant for Management Systems/
STAT DDS&T, [redacted] Records Management Officer/DDS&T, and
STAT [redacted] B Division/ODP.

The paper defines the missions and objectives of the requested system and describes the requirements that must be satisfied in order to meet the objectives. It presents an overview of the required system together with flow diagrams of major system functions. Finally, it recommends a system approach using the Generalized Information Management System (GIMS) for primary input and the National Military Command System Information Processing System (NIPS) for primary storage and retrieval.

II. MISSIONS AND OBJECTIVES

The purpose of the system is to provide a record of all collateral classified and compartmented material which the offices in the DDS&T receive? send to industrial and government contractors. The system must contain material prepared by DDS&T which is sent to a contractor and material prepared for DDS&T which is sent to a contractor. It will not contain material prepared by or for DDS&T which is not sent to a contractor. The material controlled by the system is for the most part documents.* The material and the data entered into the system will be referred to as "documents" and "document data" in the rest of the paper. The system will be used to verify semi-annual document inventories submitted by contractors. The system will also be used to keep track of inventory notifications and receipts in order to insure that inventory requirements are being complied with.

Tapes
Discs
Micrographics
Film
Hardware

ADMINISTRATIVE-INTERNAL USE ONLY

III. SYSTEM REQUIREMENTS

The system must be able to store and retrieve contractor, contract and document data in support of inventory processing tasks. Attachment 1 describes the data management tasks. Attachment 2 describes the inventory processing tasks. Attachment 3 describes output requirements associated with the inventory processing tasks. The files which are required by the system are described in Attachment 4.

STAT

The system must be able to handle a large volume of data. [redacted]

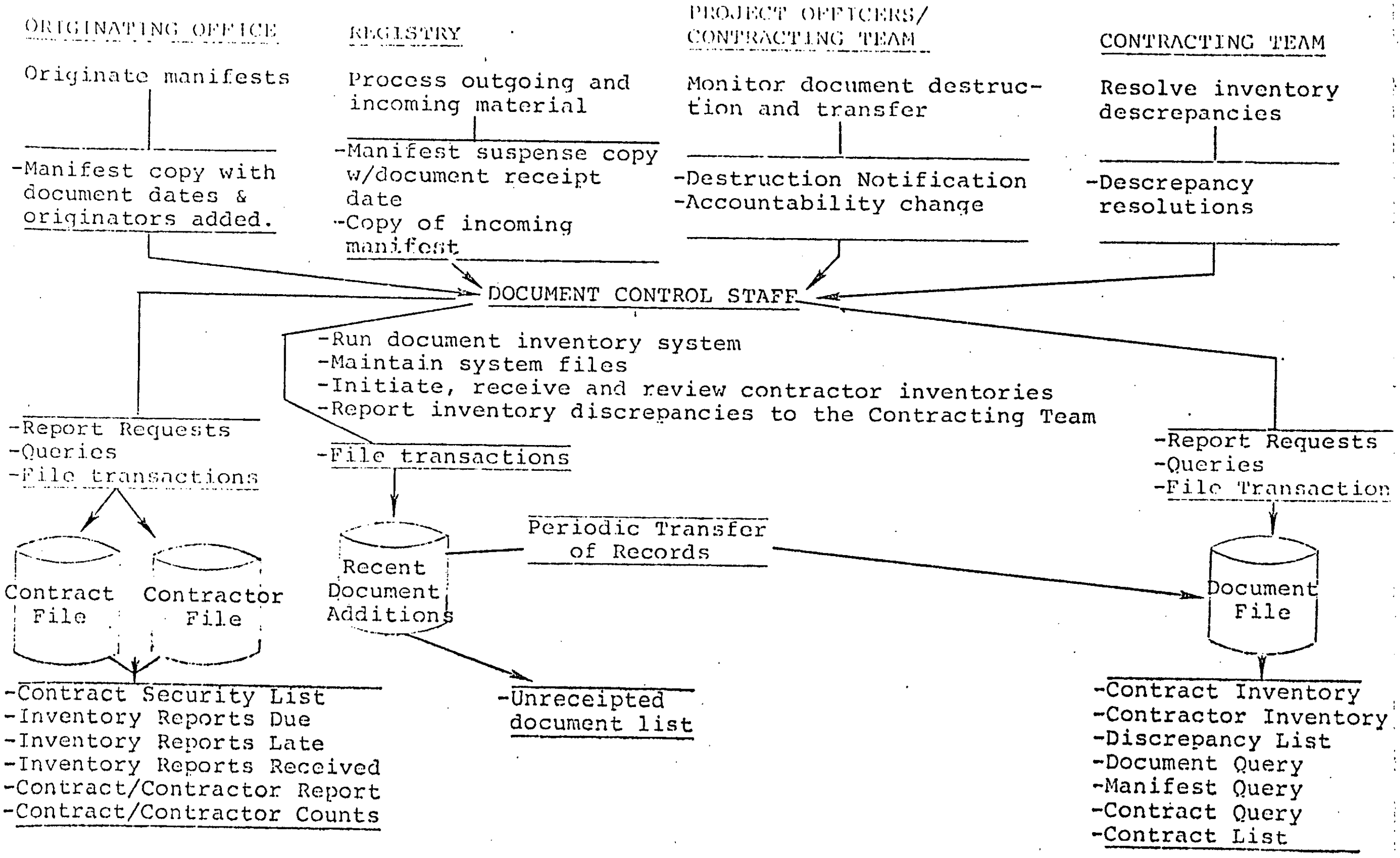
Input to the system must be via terminals with as much data validation as practical being done at input time. Report generation and file queries should produce responses in three hours or less although in most cases overnight processing will be acceptable.

The system should maintain a count of documents sent to each contractor and related to each contract.

IV. SYSTEM OVERVIEW

In Section III and its related attachments many aspects of the required system are identified and described. Attachment 1 describes the data management tasks of six office components: the originating office, the registry, the project officers, the contracting team, and the Document Control Staff. Attachment 3 describes 14 separate output requirements. Attachment 4 describes three system files: contract, contractor and document. The relationship between these components, files and outputs is shown in the system overview and flow descriptions on the following pages.

SYSTEM OVERVIEW



ORIGINATING OFFICE

Originate manifests

- Manifest copy with document dates & originators added.

REGISTRY

Process outgoing and incoming material

- Manifest suspense copy w/document receipt date
- Copy of incoming manifest

PROJECT OFFICERS/ CONTRACTING TEAM

Monitor document destruction and transfer

- Destruction Notification
- Accountability change

CONTRACTING TEAM

Resolve inventory descrepancies

- Descrepancy resolutions

DOCUMENT CONTROL STAFF

- Run document inventory system
- Maintain system files
- Initiate, receive and review contractor inventories
- Report inventory discrepancies to the Contracting Team

- Report Requests
- Queries
- File transactions

Contract File

Contractor File

- Contract Security List
- Inventory Reports Due
- Inventory Reports Late
- Inventory Reports Received
- Contract/Contractor Report
- Contract/Contractor Counts

- File transactions

Recent Document Additions

Periodic Transfer of Records

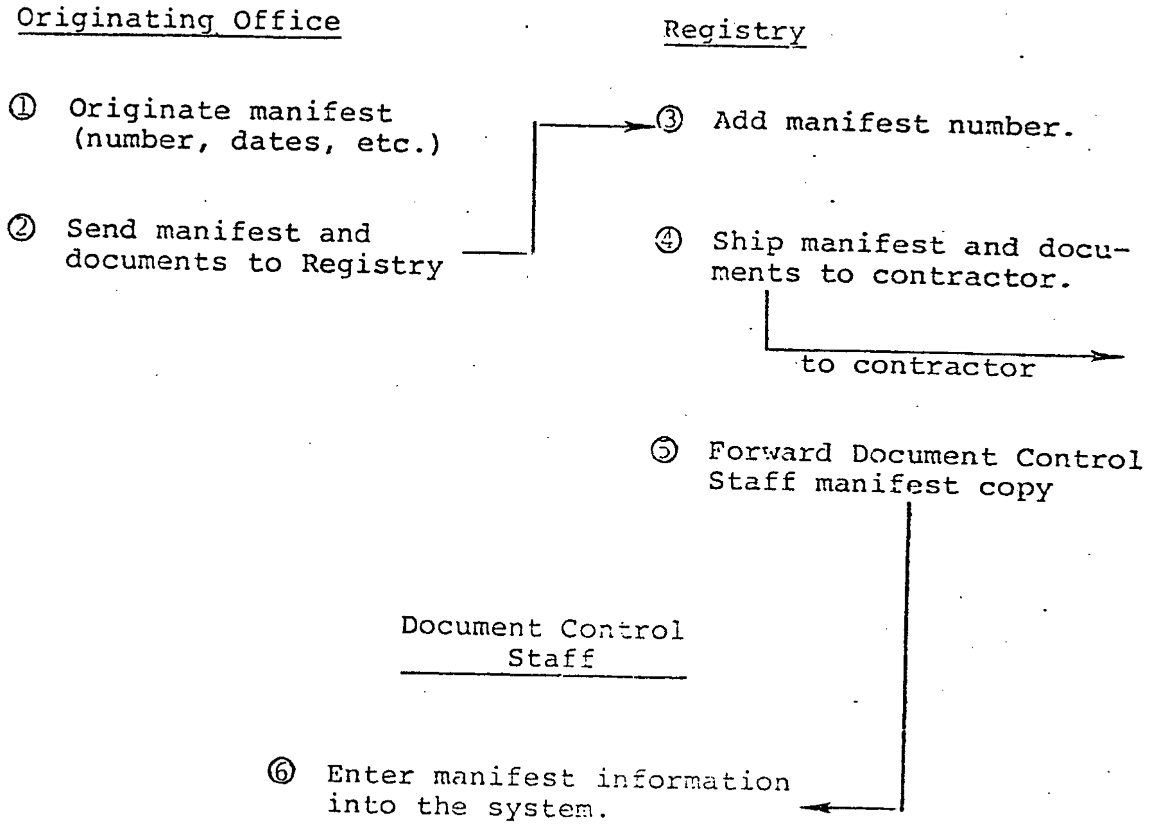
- Unreceipted document list

- Report Requests
- Queries
- File Transaction

Document File

- Contract Inventory
- Contractor Inventory
- Discrepancy List
- Document Query
- Manifest Query
- Contract Query
- Contract List

OUTGOING DOCUMENT PROCESSING



Originating Office

① Originate manifest (number, dates, etc.)

② Send manifest and documents to Registry

Registry

③ Add manifest number.

④ Ship manifest and documents to contractor.

to contractor

⑤ Forward Document Control Staff manifest copy

Document Control Staff

⑥ Enter manifest information into the system.

ADMINISTRATIVE-INTERNAL USE ONLY

RECEIPTED MANIFEST PROCESSING

Registry

① Receive receipted manifest from the contractor.

② Send manifest copy to Document Control Staff.

④ File receipted manifest

Document Control Staff

③ Enter document receipt information into the system.

ADMINISTRATIVE-INTERNAL USE ONLY

INCOMING DOCUMENT PROCESSING

Registry

① Receive incoming documents and contractor manifest.

② Send manifest copy to Document Control Staff. indicating which items had [illegible] sent to the contractor eg DDS&T

④ Return receipted manifest to contractor.

→ to contractor

Document Control Staff

③ Enter document transmittal information into the system.

ACCOUNTABILITY TRANSFER PROCESSING

Project Officer/Contracting Team		Document Control Staff
① Receive report of accountability transfer from the contractor.	→	② Enter document transfer information into the system.

ADMINISTRATIVE-INTERNAL USE ONLY

DOCUMENT DESTRUCTION PROCESSING

Project Officer/Contracting Team		Document Control Staff
① Receive document distruction notification from the contractor.	→	② Enter document destruction date and authorization into the system.

MANAGE INVENTORIES

Document Control Staff

① List late inventory reports.

② Send late notices. to contractor →

③ List inventories due.

④ Send inventory notifications. to contractor →

⑤ Enter notification date into the system.

⑥ Produce list of inventories due.

⑦ Produce list of late inventories.

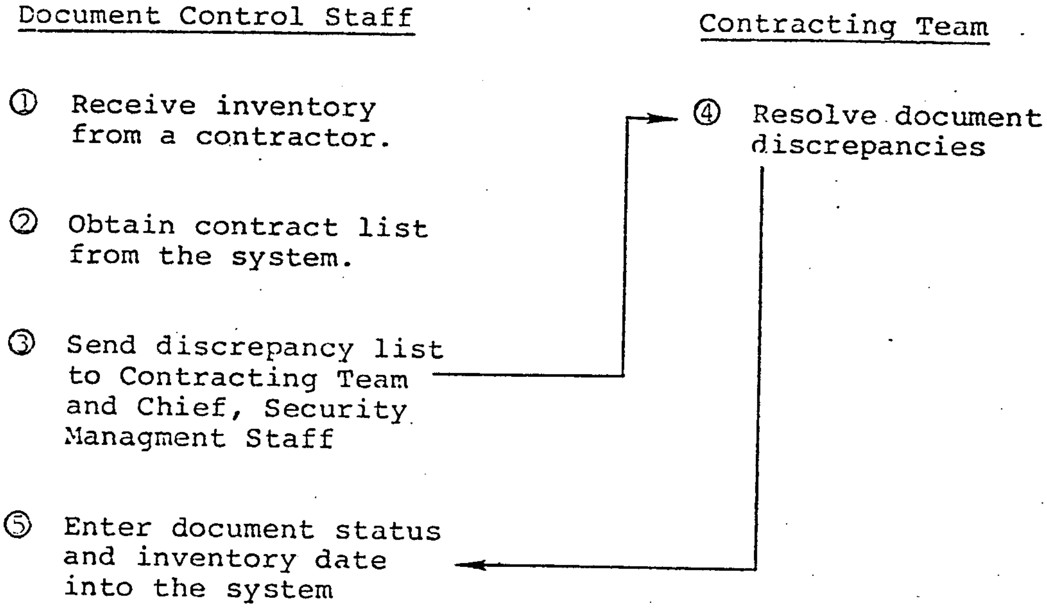
⑧ For closed contracts list all documents with unresolved status.

⑨ Send ⑥, ⑦ and ⑧ for individual offices to the Contracting Team and the office registry.

⑩ Sent ⑥, ⑦ and ⑧ for the Directorate to Chief, Procurement Staff and Chief, Security Management Staff.

⑪ Produce unreceipted document list for each registry.

PROCESS INVENTORIES



Document Control Staff

① Receive inventory from a contractor.

② Obtain contract list from the system.

③ Send discrepancy list to Contracting Team and Chief, Security Managment Staff

⑤ Enter document status and inventory date into the system

Contracting Team

④ Resolve document discrepancies

V. RECOMMENDATION

The requirements defined in Section III and summarized in Section IV can be satisfied using ODP's two information management systems: GIMS - Generalized Information Management System and NIPS - National Military Command System Information Processing System. GIM would be used for the online (via terminal) input of document, contract and contractor data. GIM would be able to provide the required level of input time editing. GIM would produce all output required from the contract and contractor files. Contract and contractor data would be stored online in GIM files. Document data will initially be stored in a GIM file but will be moved periodically to a large NIPS file.

The large volume of data in the document file, the three hour response time, and the report requirements are well suited to the NIPS system. NIPS would be used for the storage and retrieval of document data. NIPS would produce the inventory reports and process the queries against the document file.

ATTACHMENTS

ATTACHMENT 1

DATA MANAGEMENT TASKS

OUTGOING

Originator

- Enter manifest information
- Send documents and manifest to Registry

Manifest & Documents

Registry

- Assign manifest number
- Stamp documents with special symbol
- Check manifest and correct errors where possible
- Package and send the material
- Retain one copy of manifest (Suspense copy)
- Forward Document Control Staff copy

DCS Manifest copy

Document Control Staff (DCS)

- Enter document information via terminal
- Destroy DCS manifest copy

INCOMING

Document Control Staff (DCS)		Registry
		Receipted Manifests
		- Pull suspense copy, add any corrections, add date received and mark receipted.
- Enter receipt information via terminal	← suspense copy	- Forward suspense copy to Document Control Staff.
- Destroy suspense copy		- File receipted manifest.
		Returned Documents
		- Validate incoming manifest
		- If a document has the special symbol, stamp the special symbol on the manifest next to the document entry.
		- Copy incoming manifest
- Enter transmittal information for returned items via terminal	← incoming manifest copy	- Forward copy to DCS
		- Return receipted manifest to sender.
- Destroy manifest copy		

OTHER

Project Officer/Contracting Team		Document Control Staff (DCS)
- Receive document destruction information		
- Notify DCS of document destruction	Destruction Notification →	- Enter destruction data and authorization via terminal
- Receive report of accountability transfer		
- Notify DCS of accountability transfer	Accountability Change →	- Enter transfer data via terminal

ADMINISTRATIVE-INTERNAL USE ONLY

ATTACHMENT 2

INVENTORY PROCESSING TASKS

-Administer inventory system.

1) Obtain Inventory Reports Due listing

2) Send inventory requests to contractors.

   a) Record notification date (CONTRACT).

3) Obtain Inventory Reports Late listing.

4) Send inventory late notices to contractors.

5) Send Inventory Reports Due and Inventory Reports Late, by office, to the Contracting Team and the office registry, by directorate to, Chief, Procurement Staff, and Chief, Security Management.

6) For closed contracts list all documents with unresolved status. (Send list to same groups as in 5).

-Process incoming inventories

1) Record date inventory received (CONTRACT).

2) Obtain Contract Inventory or Contractor Inventory.

3) Review inventories.

4) Create discrepency list for Contracting Team and Chief, Security Management Staff.

5) Record document status (DOC) and inventory date.

-Follow up on discrepencies

1) Obtain Discrepency List.

2) Resolve outstanding discrepencies with Contracting Team and record document status (DOC).

ADMINISTRATIVE-INTERNAL USE ONLY

-Obtain Inventory Reports Received listing by office for the Contracting Teams and the Registries and for the Directorate for Chief, Procurement Staff and Chief, Security Management Staff.

-Obtain Unreceipted Documents List for each registry.

ATTACHMENT 3

OUTPUT REQUIREMENTS

Output from the Doc File

Contract Inventory - For a given contract list: document number, document type, document date, classification, subject, responsible office, source, each subset with copies, status, status date, inventory date, comments, each transfer, with transfer identifier, transfer type, from, to, sent data, receipt date.

Contractor Inventory - For contracts sorted within contractor list the same information as in the Contract Inventory.

Discrepancy List - For a given status, list documents sorted by contract showing the same information as in the Contractor Inventory.

Document Query - List all data related to a given document or range of documents.

Manifest Query - List all documents for a given manifest or group of manifests. Same information as in the Contract Inventory.

Contract Query - For a given contract list all documents with a given status showing the same information as in the Contract Inventory.

Contract List - For a given contract list all documents sorted by status showing the same information as in the Contract Inventory.

Unreceipted Documents List - List all documents which have no received date and which were sent more than 20 days prior to the current date. List document number, document type, classification, subject, sent date.

Output from the Contract File

Contract Security Listing - Sorted list by contract within contractor within responsible office showing authorized classification.

Inventory Reports Due - Sorted list by contract within contractor showing next inventory due date, contract status, status date and audit date. Selection on due date.

Inventory Reports Late - Sorted list by contract within contractor showing notification date.

Inventory Reports Received - Sorted list by contract within contractor within office showing notification date and received date. Selection on received date.

Contract Report - Sorted list by contract within contractor within responsible office showing all contract file information.

Contractor/Contract Counts - Produce a listing by contract within Contractor showing the number of documents held. The listings may be requested for a single contract, a single contractor, or all contractors.

ATTACHMENT 4

FIELD DESCRIPTIONS AND DATA FORMAT SPECIFICATIONS

The following sections are a detailed description of the main files:

1. Field Descriptions:

FIELD	MAX LENGTH	DESCRIPTION
DOC:		
DOC	35	Document Number
TYPE	2	Type of document
DOC/D	4	Document date
SOURCE	20	Source of document
SYS	3	Control system
CLASS	2	Classification
COUNT	0	Field to generate contract and contractor counts
SUBJECT	200	Document subject
SUBSET	15	Document subset ID

(The following fields describe a subset)

FIELD	MAX LENGTH	DESCRIPTION
COPIES	3	Number of copies
DESTROY/D	4	Date documents destroyed
AUTH	20	Destruction authorization
DSTATUS	1	Status of the subset
INV/D	4	Date subset last inventoried
CONTRACT	23	Contract number
CONTRACTOR-CODE	5	Contractor code
COMMENTS	200	Comments
TRAN-GROUP	63	Transmittal group

(TRAN, TRANT, FROM, TO, SENT/D, RECD/D are segments of TRAN-GROUP)

FIELD	MAX LENGTH	DESCRIPTION
TRAN	13	Transmittal number
TRANT	2	Transmittal type
FROM	20	Sender
TO	20	Receiver
SENT/D	4	Date sent
RECD/D	4	Received date

ADMINISTRATIVE-INTERNAL USE ONLY

ADMINISTRATIVE-INTERNAL USE ONLY

FIELD	MAX LENGTH	DESCRIPTION
CONTRACT-LIST		
CONTRACT-LIST	23	Contract number
CONTRACTORS	20	Contractor name
CSTATUS	1	Contract status
STATUS/D	4	Status date
NOTE/D	4	Inventory notification date
REC/D	4	Date inventory received
AUDIT/D	4	Date of last physical audit
NEXTI/D	4	Date of next inventory
CLEAR	20	Authorized classification
RESP	5	Responsible office
COUNTA	6	Document count
CONTRACTOR-LIST		
CONTRACTOR-LIST	20	Contractor name
CONTRACTS	23	Contract numbers
COUNTB	6	Document count
C-CODE	5	Contractor code
STREET	40	Street
CITY	20	City
STATE	5	State
ZIP	5	Zip code

2. Data Format Specifications

DOC File:

° DOC - Unique document number

Length: 35

Format: SYS/DESIG-NUM-YR/TIE

STAT

SYS : (3) Control system

/DESIG: [redacted]

-NUM : (22) Up to 21 characters. The field may also contain dashes (-) and slashes (/). (Required)

-YR : (3) 2 digit year (Required).

/TIE : (3) Special identifier used to relate documents. This field is optional.

ADMINISTRATIVE-INTERNAL USE ONLY

Edit Check: Validate SYS

Examples : [redacted]

STAT

Comments : Required

° TYPE - Type of document

Length: 2

Format: AA

AA:	CL	Computer Listing
	DR	Drawing
	EQ	Equipment
	FI	Film
	MF	Microfilm of Fiche
	MO	Model
	MT	Magnetic Tape
	PA	Paper - Memo, Report, etc.
	PH	Photographs
	TC	Tab Cards

Edit Check: Must be a valid code.

Comments: Required

° DOC/D - The date on the document

Length: 6

Format: Numeric MMDDYY

Edit Check: Valid date

Comments: Required

° SOURCE - The originator of the document if other than the disseminating office.

Length: 20

Format: Alphabetic

° SYS - System in which the document in controlled.

Length: 3

Format: Alpha

Comments: Same as the SYS segment of DOC. Required.

° CLASS - Document classification.

Length: 2

Format: AA

AA:

C	Confidential
S	Secret
TS	Top Secret
U	Unclassified

Edit Check: Must be C, S, TS, or U.

Comments: Required

° SUBJECT - Document subject.

Length: 210

Format: Alphanumeric

Comments: Required

° SUBSET - Copy number or some other unique identifier.

Length: 15

Format: Alphanumeric

Examples: CPY1
CPY1-250
CPY3-SER-AB
ALL

Comments: This field defines a subset of a set of documents. All the fields which follow are associated with this identifier. This field may repeat. Required.

° COPIES - Number of copies transmitted.

Length: 3

Format: NNN

Edit Check: Numeric

Comments: This field may repeat. Entries should remain in the order they are entered. (Required)

° DESTROY/D - The date the documents were destroyed.

Length: 6

Format: Numeric MMDDYY

Edit Check: Valid date

° AUTH - Name of official that authorized destruction of the documents.

Length: 20

Format: Alphabetic

Comments: Required when DESTROY/D is entered.

° DSTATUS - Status of transmittal group document subset.

Length: 1

Format: A

A: D - Destroyed
R - Returned
T - Transferred
S - Security
C - Contractor
K - Authorized retention (KEPT)
O - Transferred out of our security system.

Comments: Required

° INV/D - Last date that the documents subset was verified against an inventory.

° CONTRACTOR-CODE - 5 digit code obtained automatically form the CONTRACTOR-LIST file.

Length: 5

Format: Numeric

Length: 6

Format: Numeric MMDDYY

Edit Check: Valid date

- CONTRACT - Contract with which the subset is associated.

Length: 23

Format: Alphanumeric

Edit Check: Verify against the CONTRACT-LIST file.

Comments: Required

- COMMENTS - Comments about a document subset.

Length: 200

Format: Alphanumeric

- TRAN - Transmittal number, manifest number.

Length: 13

Format: AAAA-NNNNN-YY

Example: OD&E-01234-77

Comments: This field defines a transfer of a document subset. The following five fields TRANT,FROM,TO,SEND/D,RECD/D are related to TRAN. All five fields may repeat. Required.

- TRANT - Transmittal type

Length: 2

Format: Alphabetic

Edit Check: Must be a valid type:

[redacted]

STAT

Comments: Required when TRAN is filled in.

° FROM - The originator of the document transfer.

Length: 20

Format: Alphanumeric

Edit Check: Validate against the contractor list.

Comment: This field will contain the name of a contractor, government agency or DDS&T office. Required when TRAN is filled in.

° TO - The receiver of the document transfer.

Length: 20

Format: Alphanumeric

Edit Check: Validate against the CONTRACTOR-LIST file.

Comment: This field will contain the name of a contractor or DDS&T office. This field is required when TRAN is filled in.

° SEND/D - The date the document leaves "FROM".

Length: 6

Format: Numeric MMDDYY

Edit Check: Valid date

Comment: This field is required when TRANS is filled in.

° RECD/D - The date the document reaches "TO".

Length: 6

Format: Numeric MMDDYY

Edit Check: Valid date

CONTRACT-LIST File:

° CONTRACT-LIST: A unique contract number.

Length: 23

Format: Alphanumeric

° CONTRACTOR - Contractor names

Length: 20

Format: Alphanumeric

Edit Check: Must be in the contractor file.

Comment: This field may repeat. Required.

° CSTATUS - Contract status

Length: 1

Format: A

A: R - RFP
A - Active
C - Closed

Edit Check: Must be a valid character. Required.

° STATUS/D - Date of contract status

Length: 6

Format: Numeric DDMMYY

Edit Check: Valid date

Comment: Required

° NOTE/D - Date notification sent to contractor that next inventory is due.

Length: 6

Format: Numeric DDMMYY

Edit Check: Valid date

° REC/D - Date inventory received from a contractor.

Length: 6

Format: Numeric DDMMYY

Edit Check: Valid date

° AUDIT/D - Date of the last physical audit.

Length: 6

Format: Numeric DDMMYY

Edit Check: Valid date

° NEXTI/D - Date of the next inventory.

Length: 6

Format: Numeric DDMMYY

Edit Check: Valid date

° CLEAR - Authorized classification level for the contract.

Length: 20

Format: Alphabetic

Edit Check: Validate against a classification table.

Comments: Required

° RESP - Responsible office

Length: 5

Format: Alphabetic

° COUNTA - Contractor document count

Length: 6

Format: Numeric

CONTRACTOR-LIST File:

- CONTRACTOR-LIST - Contractor name

  Length: 20

  Format: Alphanumeric

- C-CODE - Contractor code

  Length: 5

  Format: Numeric

  Comments: Input to CONTRACTOR-CODE field in DOC

- STREET - Street address

  Length: 40

  Format: Alphanumeric

- CITY - City

  Length: 20

  Format: Alphanumeric

- STATE - State

  Length: 5

  Format: Alphabetic

- ZIP - Zip code

  Length: 5

  Format: Numeric

- CONTRACTS - Contract numbers

  Length: 23

  Format: Alphanumeric

  Comments: This field joint stored from the CONTRACT-LIST file.

- COUNTB - Contractor document count.

  Length: 6

  Format: Numeric

STAT

Next 1 Page(s) In Document Exempt

ISSUES AND RECOMMENDATIONS

I. ISSUE: Should the processing of inventories and the maintenance of the contractor inventory document system be additional functions of the directorate Records Management Officer?

BACKGROUND: The following is the workload per office to maintain the document file.

Man-Hours Per Week

STAT

[redacted]

Processing inventories will require another 74 hours a week. Inventory processing will consist of:

a) Notifying contractors when inventories are due.

b) Notifying contractors when inventories are late.

c) Verifying 2000 inventories per year.

d) Resolving inventory descrepancies.

e) Reflecting inventory results in the document and contract files.

f) Providing the Contracting Teams, Chief, Procurement Staff, Chief, Security Management Staff with inventory status and discrepancy information.

There are two approaches to the management of the new inventory system. A centralized approach would place both the document file maintenance and inventory processing under the control of the DDS&T Records Management Officer. This approach would require two people to do data input and two people to do inventory processing. A fifth person would be required for (part-time) management and administration of the group. Clerical support would come from the DDS&T Registry. An alternative approach would be to partially decentralize the data input function and make it a function of the office registries. The partially decentralized approach would require two additional people in ODE to do ODE's data input. In addition there would have to be at least one individual in OSO and ORD to do their input on a part-time basis. [redacted] STAT NPIC and OTS would be done in the DDS&T Registry. The partially decentralized approach would require Three additional people in the DDS&T Registry to do inventory processing and administration plus the part-time input task.

The manning requirements for the two alternatives can be summarized as follows:

	Centralized	Decentralized
[redacted]		

RECOMMENDATION: The centralized approach is recommended because it requires fewer trained people and will give the Records Management Officer greater control over all the system elements.

II. ISSUE: How should we obtain records of the documents currently at the active contractor sites?

BACKGROUND: Each office has been asked to determine the status of their records of documents sent to a contractor. All offices except ODE have reported a lack of complete document records for documents sent prior to 1973. OTS has reported that it has no historical data that can be entered into the system. ODE has indicated that they are not able to associate historical document records with specific contracts. The lack of contract association is a problem. To provide for the most efficient processing of inventories, especially in the case of large contractors, documents should be able to be grouped by contract number. If documents can only be grouped by contractor it is likely that some contractors will have 30,000 associated documents. Lists with this many entries will be difficult to use for inventory verification.

We have discussed the possibility of performing an inventory of contractor held documents with the DDS&T Security Staff, Office of Logistics industrial security personnel, and with the DDS&T Chief Contracting Officer. All feel that contractors should be able to provide copies of their classification material logs. There is doubt, however, as to whether the logs will be complete for old documents or for documents relating to closed contracts. Regarding inventories, the assessment was that contractors holding a small number of documents would willingly respond to an inventory request. Contractors holding a large number of documents would have a problem responding to an inventory request. There was uncertainty as to whether or not contractors would require additional funds to perform the inventory function.

RECOMMENDATION: Due to the lack of complete office data we should request that contractors provide us with an inventory of documents that they have received from us or a copy of their Master Control Logs. The logs and inventories should be reviewed and prepared for input. The cost of the review and preparation can only be determined after we have seen samples of the logs and inventories. We expect that inventories submitted according to the recently defined DDS&T Inventory Guidelines will require very little preparation. Copies of contractor logs will require more time to review and prepare.

III. ISSUE: How should we treat data related to closed contracts and inactive contractors?

BACKGROUND: There are many contractors who have kept documents after their contracts have been closed. There are also contractors that have safes and vaults full of material for which they have no further use. In the past, contractors have been authorized to keep documents in anticipation of future requirements after a contract has been closed. Our discussions with contracting and security personnel indicate that in many cases records of the retained material do not exist. A review of several closed contract folders has failed to turn up any of the required document logs which are supposed to indicate the dispostion of documents at the close of the contract.

Members of the Industrial Contractor Inventory Task Force have indicated that a request for return of material unrelated to open contracts will result in truck loads of documents being returned to the Agency. The proper review and disposition of this material is expected to be a very costly project. A less costly alternative would be to arrange for review and disposition at the contractor's site.

RECOMMENDATION: Each inactive contractor should be notified to submit an inventory of their holdings or arrange for proper disposal. Only documents that we authorize them to keep and for which we retain the responsibility should be entered into the system.

The cost of review and disposition of this old material cannot be determined until we begin to receive responses from the contractors.

STAT

Next 1 Page(s) In Document Exempt

PLAN TO CAPTURE HISTORICAL DATA

I. Obtain records of current contractor document holdings.

A. Estimate current holdings by contract and contractor for open contracts.

B. Request contractors to provide us with an inventory of their holdings.

II. Input Historical Data

A. Review contractor lists and deliver to central input point.

B. Key data to disk (IV Phase system)

C. Move data from disk to NIPS data file.

III. Data To Be Captured

Document Number*

Document Type*

Classification

Copy Description

Number of copies

Subject

Contract number*

Sender (office)

Manifest number

Date sent or date received*

Contractor recipient*

Document date

* These fields are required.