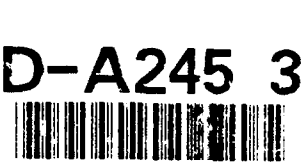


(2)

NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

IMPROVED CLASSSIFIED MATERIAL CONTROL THROUGH THE APPLICATION OF A DATABASE MANAGEMENT SYSTEM

by

Terrance Clifford Brady

September 1991

Thesis Advisor: Myung W. Suh

Approved for public release; distribution is unlimited

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b OFFICE SYMBOL (*If applicable*) 37	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000	7b ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000
8a NAME OF FUNDING/SPONSORING ORGANIZATION 8b OFFICE SYMBOL (*If applicable*)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (*City, State, and ZIP Code*)	10 SOURCE OF FUNDING NUMBERS Program Element No / Project No / Task No / Work Unit Accession Number

11 TITLE (*Include Security Classification*)
IMPROVED CLASSIFIED MATERIAL CONTROL THROUGH THE APPLICATION OF A DATABASE MANAGEMENT SYSTEM

12 PERSONAL AUTHOR(S) Brady, Terrance C.

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (*year, month, day*)	15 PAGE COUNT
Master's Thesis	From To	September 1991	143

16 SUPPLEMENTARY NOTATION
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17 COSATI CODES			18 SUBJECT TERMS (*continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUBGROUP	Classified Material, Database Management System, DBMS

19 ABSTRACT (*continue on reverse if necessary and identify by block number*)

Most military organizations maintain classified material but systems of accountability vary from one command to another. This thesis presents the design and implementation of a prototype database system, called COMMANDOC, that provides an automated mehtod of tracking these documents including subcustody to a secondary control point, check out to an individual user, transfer to a new command, and destruction. All required reports are generated by the system. In addition to the information on the actual documents, the database contains information on the personnel authorized to use both the documents and to operate the system, thereby ensuring only personnel with the necessary access are allowed to check out documents. A password system ensures only authorized personnel utilize the system, and a weekly audit report of system users is provided to the supervisor. The system provides a simple menu interface that leads the user through each step of a transaction and a user's manual is provided.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION	
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS REPORT ☐ DTIC USERS	UNCLASSIFIED	
22a NAME OF RESPONSIBLE INDIVIDUAL Myung W. Suh	22b TELEPHONE (*Include Area code*) (408) 646-2161	22c OFFICE SYMBOL AS/SU

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

Approved for public release; distribution is unlimited.

Improved Classified Material Control Through The Application
of a Database Management System

by

Terrance Clifford Brady
Major, United States Marine Corps
B.B.A., National University, 1984

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1991

Author: _____
Terrance Clifford Brady

Approved by: _____
Myung W. Suh, Thesis Advisor

_____
Magdi Kamel, Second Reader

_____
D. R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

Most military organizations maintain classified material but systems of accountability vary from one command to another. This thesis presents the design and implementation of a prototype database system, called COMMANDOC, that provides an automated method of tracking these documents including subcustody to a secondary control point, check out to an individual user, transfer to a new command, and destruction. All required reports are generated by the system. In addition to the information on the actual documents, the database contains information on the personnel authorized to use both the documents and to operate the system, thereby ensuring that only personnel with the necessary access are allowed to check out documents. A password system ensures only authorized personnel utilize the system, and a weekly audit report of system users is provided to the supervisor. The system provides a simple menu interface that leads the user through each step of a transaction and a user's manual is provided.

TABLE OF CONTENTS

I. INTRODUCTION

A. BACKGROUND

Virtually every military organization must at some time create or at least have access to classified material in order to accomplish its mission. Some organizations (combat units, for example) depend on classified material more than others (such as garrison training commands). However, wherever classified material is used, certain procedures must be followed for its proper control and accountability. For the Department of the Navy, these procedures are set forth in OPNAVINST 5510.1H, Department of the Navy Information and Personnel Security Program Regulation.

Because of the varied nature of the many organizations throughout the Department of the Navy, OPNAVINST 5510.1H provides only broad principles for control and accountability, leaving much latitude to local commanders to implement their security programs in a manner best suited for the local environment. While accountability is provided, the procedures are not standardized. This can create some confusion when an individual responsible for the daily operations of classified material security moves from one location to another.

B. OBJECTIVES

The objective of the thesis was to design and implement a prototype database system for tracking classified document. The prototype, called the **COM**mand **MAN**agement of

Classified **DOC**uments (COMMANDOC), was created to provide some standardization to this process and to utilize commonly available personal computers to assume most of the drudgery of the mundane, routine record keeping. It is a fast, efficient, and convenient system that improves the accuracy of record keeping while enhancing managerial control of classified material. The system will satisfy the record keeping requirements of existing directives and provide accurate and uniform reports. COMMANDOC will also assist in the emergency destruction planning for classified documents by providing up-to-date inventories of each drawer of material in each safe.

The managerial requirements built in to the system will require active participation by the Classified Material Control Center Officer (CMCC Officer), but will not be burdensome. It will tell the custodian what he needs to know about his account and keep him abreast of the activities he should be involved in.

C. THE RESEARCH QUESTION

The research question is "How can a personal computer and data base management system be utilized to provide a common system of control for classified documents in Marine Corps activities?" While no one system may be perfect for every application, this thesis presents a balanced answer that should prove acceptable to most, if not all, environments.

D. SCOPE, LIMITATIONS, AND ASSUMPTIONS

The scope of this control system was designed to maintain unclassified accounting of classified documents. That is, this system does not provide protection to classified material--it performs the unclassified function of tracking those items which are classified. Classified titles of documents, for example, must not be entered into the COMMANDOC system. To do so will cause the computer to become classified. Situations which need to enter classified titles must comply with existing regulations, both local and higher headquarters.

E. LITERATURE REVIEW AND METHODOLOGY

A literature review was conducted of existing documents to compile the requirements for a classified material control system. The existing paper-based model was generally followed, but using the power of the personal computer whenever possible to reduce the workload. Paper forms that are required matched the output of the system, and facsimiles of general purpose forms are recreated by the system on plain paper in order to avoid loading and reloading of different types of paper. The methodology of the research was based upon this review of existing directives, review of the current system at the Naval Postgraduate School, and the personal experiences of the author as a CMCC Custodian.

F. DEFINITIONS AND ABBREVIATIONS

The nature of this study lends itself to many abbreviations. A complete list of abbreviations can be found in Appendix A.

G. ORGANIZATION OF STUDY

Chapter II, Background, discusses the operations of a typical CMCC. The types of documents, access, and reports are examined as they exist in a manual based system.

Chapter III, User Requirements for COMMANDOC, presents the methodology used for the system and describes the various objects the comprise a typical operation.

Chapter IV, COMMANDOC System Design, provides a discussion of the overall system. This could be considered a layman's explanation of Chapters II and III, contrasting how the objects defined in Chapter III interact and perform the actions of a common CMCC described in Chapter II. The two phases of system design, logical data base design and application design, are discussed as they apply to the COMMANDOC.

Chapter V, Conclusions, provides a brief summary of the problems encountered during the process of creating the COMMANDOC system and the lessons learned. The possibility of future versions of the system are also discussed.

The Appendix section provides a glossary of abbreviations (Appendix A), a listing of object and domain

definitions (Appendices B and C) for the objects discussed in Chapter III, and a User's Guide (Appendix D).

II. MANAGEMENT OF CLASSIFIED MATERIAL

A. TYPICAL OPERATIONS

All classified material destined for a particular organization is routed to a central clearing office, called the Classified Material Control Center (CMCC). This is normally a vault or strongroom in a designated area of the organizations headquarters element. Access is restricted to the personnel who work in the CMCC and to others on an access list authorized to enter. A CMCC Custodian and (usually) one or more CMCC Clerks are assigned to process material received at the CMCC.

In the CMCC, classified material is received and entered into an accounting system. These documents are classified top secret, secret, or confidential. They are routed as necessary and stored in locked safes when not in use. Each safe has one or more drawers. In large organizations where large amounts of documents are routinely required in an office that needs constant access to them, a Secondary Control Point (SCP) may be designated. An SCP is like a branch office of the CMCC, subordinate to it and responsible for administrative control and physical security of all documents sub-custodied to it. Like a CMCC, it has a custodian assigned to it.

If the organization is authorized to handle top secret material, a Top Secret Control Officer (TSCO) is also

assigned. He is responsible for the accountability and safeguarding of top secret documents.

1. Small Operations

A small CMCC operation is characterized by a low number of documents (probably two two-drawer safes with up to 500 documents), and no Secondary Control Points. One clerk is normally assigned full- or part-time, and a CMCC Custodian assigned as an additional duty. Neither of these billets are normally specified on the organization's Table of Organization (T/O). It normally does not maintain any top secret documents. Typical organizations in this category are infantry battalions, aviation squadrons, and similar size units.

2. Medium Operations

Medium CMCC operations are characterized by a moderate number of documents (500 to 5,000 documents stored in possibly as many as five four-drawer safes), one or more Secondary Control Points, and two or more clerks assigned on a full time basis. The staff may also include a staff noncommissioned officer (CMCC NCOIC) to supervise the daily operation of the CMCC, and a CMCC Custodian assigned as an additional duty. It may maintain a small number of top secret documents. Some of the responsibilities are specified on the T/O (often as additional duties), but additional staffing is often provided as required. Typical

organizations include infantry regiments, aviation groups, and equivalent size units.

3. Large Operations

Large CMCC operations are characterized by a large number of documents (over 5,000 documents in numerous safes), multiple Secondary Control Points, and numerous independent users authorized to maintain their own documents external to a CMCC's or SCP's control. The office may be staffed with one or more staff noncommissioned officers and several clerks, and may have a CMCC Custodian assigned as a primary duty. The CMCC may be required to operate extended hours (possibly even 24 hours a day) depending upon the mission and current operations of the command. A large CMCC is usually identified as a separate section on the T/O with dedicated manning. It maintains a moderate amount of top secret documents. Typical organizations include infantry division, aviation wing, and Force level commands.

B. ACCOUNTABILITY OF DOCUMENTS

1. Top Secret

The responsibility for accountability of top secret documents is normally assigned to a Top Secret Control Officer (TSCO). Records pertaining to top secret documents must be retained for five years after their destruction or transfer, as compared to two years for documents of lesser classification. Top secret documents must also be accounted for page by page. Page checks are not required for lesser

classified documents. A continuous chain of receipts and hand-to-hand transfer is required in addition to disclosure record that must be completed by every person who sights a top secret document. While OPNAVINST 5510.1H requires an annual inventory of top secret documents, most commands impose a semi-annual requirement.

2. Secret

The responsibility for accountability of secret and confidential material is normally assigned to a Classified Material Control Center (CMCC). Records pertaining to secret documents must be maintained for two years after their destruction or transfer. Although a page count is not required by OPNAVINST 5510.1H for secret documents, this option is available in the COMMANDOC should special circumstances warrant it. While OPNAVINST 5510.1H does not specify a schedule for inventorying secret documents, most commands establish a requirement for inventory every six months and whenever a change of custodian is effected. Although that same reference does not require signed receipts for secret documents distributed within an organization, some procedure of person-to-person accountability is normally followed. This is particularly helpful when accountability must be determined for lost or missing documents.

3. Confidential

Accounting procedures for confidential material are less stringent than higher classified material. Although OPNAVINST 5510.1H does not require records of receipt, distribution, or disposition, specific circumstances or a local commander's desires may require them. One may argue, for example, that it is impossible to establish control if some type of accountability system is not used. Likewise, the lack of such an audit trail would be an obstacle if the need arose to conduct an investigation of lost (or found) classified material. Ultimately, the use of the COMMANDOC for confidential material is left to the user and his local requirements.

C. ACCESS CONTROL

After an organization provides a system of accounting for the classified material it holds, it must then provide a system to ensure that it is accessible to those individuals who need to use it. This access must be provided on a "need to know" basis. That is to say, a user must have a valid clearance for at least the level of classification as the material desired as well as have a need to see the material.

After a determination has been made that an individual must have access to classified material in the performance of his duties, a request for clearance is forwarded to the Department of the Navy Central Adjudication Facility (DONCAF). The DONCAF will respond (often taking as much as

six weeks) with authorization or denial for the requested access. In the meantime, the local commander may issue interim access if the individual's duties require prompt access.

D. REPORTS

A variety of manual reports are generated throughout the daily operation of a CMCC. A brief description of each of these reports follows.

1. Logbook

Most manual accounting systems use standard green logbooks as the primary accounting tool for classified documents. Upon receipt of a document, its control number, copy number, title, originator, and various other traits are handwritten into the logbook. When a document is transferred or destroyed, an entry is made in the appropriate column and the entire entry is lined out with a highlighter. Figure 1 is an example of such a logbook.

Creating an inventory with this type of logbook system is an extremely painstaking process at best. Each logbook must be scanned for all of its current entries and those entries must be sorted by user or Secondary Control Point (SCP) if it has been subcustodied.

2. Document Cover Page

Each document will normally have a Correspondence/ Material Control form (OPNAV 5216/10) filled out and attached. This four part carbon form provides copies to be

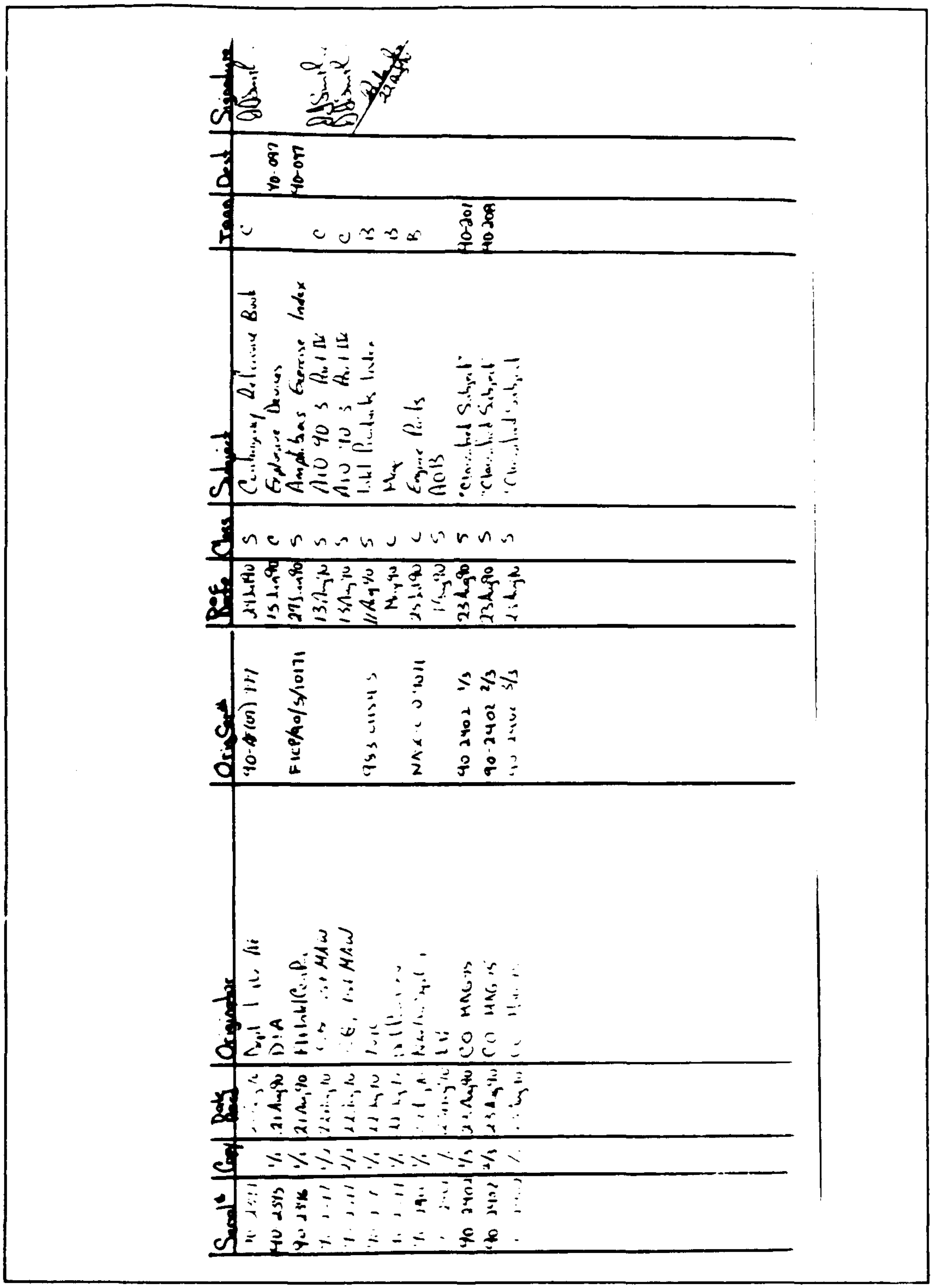


Figure 1. Sample Manual Logbook Entries.

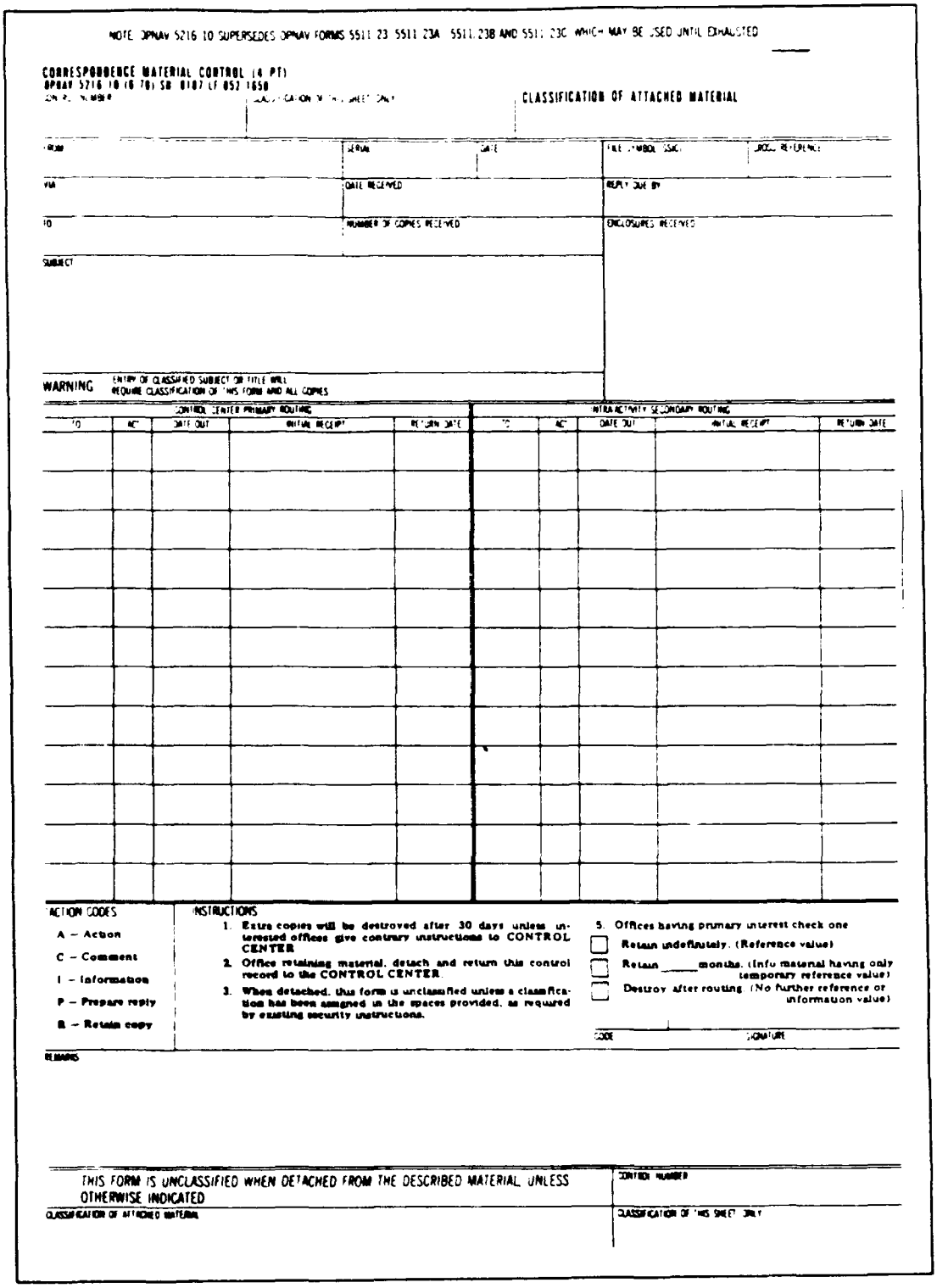
retained in a file system as well as copies for routing purposes. In existing manual systems, this form is filled out (either handwritten or typed) after the same data has been entered into the logbook. This is both a time-consuming and error-prone process. See Figure 2.

3. Inventory

A complete inventory of classified holdings is required annually, although in practice this is accomplished at least once every six months. More frequent inventories may be directed by local commanders and are also required whenever there is a change of custodian. As previously mentioned, inventories using manual systems require screening of logbooks. Other manual systems may use decks of locator cards or file copies of routing sheets (OPNAV 5216/10). Inventories must be certified by the responsible officer, returned to the CMCC, and maintained for two years (five years for top secret material).

4. Destruction Reports

Once classified material has served its purpose and serves no archival value it must be destroyed. In a typical system, the responsible officer will designate the documents to be destroyed to his clerical assistant. The clerk will list the documents on a Destruction Report form (OPNAV 5511/12). The responsible officer will sign the form to authorize the destruction, and the clerk (and an additional



NOTE: OPNAV 5216.10 SUPERSEDES OPNAV FORMS 5511/23, 5511/23A, 5511/23B AND 5511/23C WHICH MAY BE USED UNTIL EXHAUSTED

CORRESPONDENCE MATERIAL CONTROL (4 PT)
OPNAV 5216.10 (6-78) SN 0107-LF-052-1650

CLASSIFICATION OF ATTACHED MATERIAL

FROM | SERIAL | DATE | FILE SYMBOL (SSIC) | ROUTINE REFERENCE

VIA | DATE RECEIVED | REPLY DUE BY

TO | NUMBER OF COPIES RECEIVED | ENCLOSURES RECEIVED

SUBJECT

WARNING: ENTRY OF CLASSIFIED SUBJECT OR TITLE WILL REQUIRE CLASSIFICATION OF THIS FORM AND ALL COPIES

CONTROL CENTER PRIMARY ROUTING

TO	ACT	DATE OUT	INITIAL RECEIPT	RETURN DATE

INTRA-ACTIVITY SECONDARY ROUTING

TO	ACT	DATE OUT	INITIAL RECEIPT	RETURN DATE

ACTION CODES

A – Action
C – Comment
I – Information
P – Prepare reply
R – Retain copy

INSTRUCTIONS

1. Extra copies will be destroyed after 30 days unless interested offices give contrary instructions to CONTROL CENTER.
2. Office retaining material, detach and return this control record to the CONTROL CENTER.
3. When detached, this form is unclassified unless a classification has been assigned in the spaces provided, as required by existing security instructions.
5. Offices having primary interest check one
   - ☐ Retain indefinitely. (Reference value)
   - ☐ Retain _____ months. (Info material having only temporary reference value)
   - ☐ Destroy after routing. (No further reference or information value)

CODE | SIGNATURE

REMARKS

THIS FORM IS UNCLASSIFIED WHEN DETACHED FROM THE DESCRIBED MATERIAL UNLESS OTHERWISE INDICATED

CONTROL NUMBER

CLASSIFICATION OF ATTACHED MATERIAL | CLASSIFICATION OF THIS SHEET ONLY

Figure 2. Classified Material Cover Sheet.

witness, if required) will then destroy the documents (see Figure 3). Once the destruction is complete, the clerk will line out the document entries in the master logbook with a highlighter and the destruction date and report number annotated in the logbook. If the destruction is conducted at an SCP, then a copy of the destruction report will be forwarded to the CMCC. The destruction reports are maintained for two years (five years for top secret material).

5. Transfer Reports

Classified material is distributed to other organizations outside the originating command. In existing systems, this is usually accomplished in a manner similar to a destruction report. The responsible officer identifies the material to be transferred, and the clerk prepares a transfer report and packages the material for shipment to the receiving command. Upon receipt, the receiving command signs the transfer report and returns it to the sending command. The master logbook is updated with the date and transaction number of the transfer report and the entries are lined out of the logbook with a highlighter. Refer again to Figure 1.

6. Emergency Action Inventories

Each holder of classified material is required to create an emergency action plan that provides detailed

CLASSIFIED MATERIAL DESTRUCTION REPORT
OPNAV 5511/12 (REV. 8-75) S/N 0107-LF-055-1180

CLASSIFICATION *(Indicate when title or other identification is classified)*

TO:

FROM *(Name and address of activity)*

The classified material described below has been destroyed in accordance with regulations established by the Department of the Navy Information Security Program Regulation, OPNAV INSTRUCTION 5510.1E.

The purpose of this form is to provide activities with a record of destruction of classified material. Also, copies may be utilized for reports to activities originating material, where such reports are necessary.

DESCRIPTION OF MATERIAL

SERIAL OTG	ORIGINATOR	DATE	COPY NO.	LOG/ ROUTE SHEET NO.	ENCLOSURES (IDENT. & NO.)	TOTAL NO. PAGES

OFFICER OR INDIVIDUAL AUTHORIZING DESTRUCTION *(Signature, Rank/Rate/Grade)*

DATE OF DESTRUCTION

WITNESSING OFFICIAL *(Signature, Rank/Rate/Grade)*

WITNESSING OFFICIAL *(Signature, Rank/Rate/Grade)*

* U.S. Government Printing Office

Figure 3. Classified Material Destruction Report.

instructions on how to quickly transport classified material to a safe location or to destroy the classified material on hand. For example, a typhoon, flood, or civil disturbance might require relocation of material to a safer location. Eminent enemy attack or civil uprising might require destruction of the classified holdings. Part of the emergency relocation or destruction plan requires an inventory be made of the material removed or destroyed. Existing emergency action plans vary widely and change constantly as situations change.

7. Document Search

Although a search for a particular document may not require a formal report in the common sense of the term, it does require a review of the files available and an answer to an official query. In existing systems, a document search request takes two major forms:

a. Subject or Title Search

An authorized user may require access to a particular document or group of documents. The user may know the exact title of the document or may only know the general topic. More often, he may want all the documents that pertain to a particular subject.

With existing manual systems, the clerk will have to scan the latest inventory and the current logbooks for all holdings received since the last inventory. Depending upon the size of the account, this could be a very

arduous process. The process becomes even harder if the search must determine if the document in question was ever held, in which case all destruction and transfer reports must be reviewed, or possibly the lined-out entries in all the old logbooks. The process becomes impossible if the user's "keyword" is not a part of the subject line of the document.

b. Registered Mail Number Search

The second case of a document search may be required when a sending command is seeking confirmation of receipt of a shipment. The originating command will send a letter or message requesting the receipt status of a particular registered or certified mail package.

An existing system would require a manual search of registered mail records and a cross-search of that number in the logbook. While knowing the approximate date of shipment reduces the amount of searching, it is still a labor intensive process.

E. EXISTING SHORTCOMINGS

1. Manpower

While most units routinely use classified material in their operations, relatively few are staffed with full-time CMCC personnel. A Marine Corps Table of Organization (T/O) identifies each billet of each command. A review of these T/Os reveals that relatively few of them designate CMCC personnel. Most regiments and battalions within a

Division do not have specific billets for CMCC personnel. Aviation squadrons, on the other hand, usually specify an officer and a clerk, but these duties are usually assigned on an additional duty basis (i.e., the CMCC duties must be performed in addition to other regular duties).

An associated problem is the fact that many of these "part-time" workers lack a background in controlling classified material. The military occupational specialties (MOS) of those billets identified on T/Os include infantry officers, pilots, air control officers, communications officers, administration officers, administration clerks, personnel clerks, and logistics clerks. While the MOS Manual does list processing classified material as a typical duty of administrative personnel, no extensive training is provided in this area.

2. Procedures

Further shortcomings of the existing system come from the existing requirements for maintaining classified material. OPNAVINST 5510.1H provides relatively broad requirements for the security and accountability of classified material. The decentralized nature of the defined procedure results, to some degree, from the varied need of organizations throughout the Department of the Navy. While this inevitable, there are certain procedures that can be standardized and automated.

3. Investigations

Whenever a classified document is discovered lost (or accountability of the document is lost), an investigation must be conducted to determine if a compromise has occurred. In some cases, extensive man-hours will be wasted on an investigation just to determine that the "loss" was the result of an accounting error. The COMMANDOC improves the accuracy of record keeping for classified material and thereby stands to reduce the number of investigations caused by these accounting errors. In those cases where an investigation must still be accomplished, the system will speed up the process of searching records for an audit trail.

Consider the following scenario. An investigation is ordered into the reported loss of a secret document. Because the officer responsible for the document is a first lieutenant, a senior officer (a captain) is assigned to conduct the investigation. The CMCC is operated by a staff sergeant and a corporal, with a captain assigned as CMCC Officer as an additional duty. The investigating officer will have a lance corporal clerk assigned to him for typing and other clerical duties during the course of the investigation. For the purpose of determining pay and allowances, we shall assume that only the officers and the staff sergeant are married.

When an investigation is assigned to an officer it becomes his primary duty, and he normally has ten days to complete it. Assuming the officer completes this investigation in eight days, the estimated costs involved would be as follows.

ITEM	COST	TOTAL COST
Investigating officer primary duty	$3382.80 per month or $112.76 per day for 8 days	$902.08
Responsible officer time spent searching for document and preparing required statements	$2751.60 per month or $91.72 per day for 1 day	$91.72
SSgt NCOIC of CMCC time spent searching for document and researching records	$1867.20 per month or $62.24 per day for .5 day	$31.12
Cpl CMCC Clerk time spent searching for document and researching records	$1042.20 per month or $34.74 per day for .5 day	$17.37
LCpl clerk/typist time spent typing statements, investigation, making photocopies, etc.	$926.40 per month or $30.88 per day for 2 days	$61.76
TOTAL COST		$1104.05

Note: The above scenario assumes Capt over 8 years of service, 1stLt over 3, SSgt over 8, Sgt over 4, Cpl over 3, LCpl over 2. Based on 1991 military pay schedule, SSgt/above married, drawing BAQ and COMRATS/BAS.

The figures used in this scenario do not include time lost for additional personnel being interviewed, possible transportation costs (i.e., gas and cost of a driver) if the investigating officer must travel to interview additional parties, etc. The costs incurred could be higher if a more senior investigating officer must be

assigned. These costs are incurred regardless of whether or not the document is actually found.

In short, the estimated savings that could be realized for such an investigation is $1,100.

4. Recordkeeping

The current record keeping system is bulky, tedious, and error-prone. Manual entries must be made into logbooks and then lined out. Old logbooks must be kept in an active status because of a small number of active documents still recorded within them. Searches for past records are time consuming and painstaking.

F. BENEFITS OF THE COMMANDOC SYSTEM

1. Manpower

The automated procedures provided by the COMMANDOC permits an inexperienced CMCC Officer or clerk to quickly and accurately control the documents assigned to the command's CMCC account. The system forces the CMCC Officer to be involved with the account, but enhances his managerial control by quickly providing the information he needs to know in an efficient manner. This allows him to obtain better control over his account while spending less time in an already over-committed schedule. Similarly, the work performance of a clerk can be greatly improved. If an alternate clerk is assigned on an irregular basis, the COMMANDOC provides less likelihood of errors as the

alternate clerk assumes responsibility in the primary clerks absence (i.e., sick, leave, emergency leave, etc.).

2. Procedures

The standardized system COMMANDOC permits standardized training and inspecting procedures. Since all units will use the same system, a clerk or custodian transferring from one unit to another would have less learning time spent on the new organization's methodology. An intangible benefit would be realized through this time savings, as well as the benefits of less storage space for bulky logbooks and more accurate record keeping. Clerical errors from transposed or missing control numbers would be eliminated.

3. Investigations

One goal of the COMMANDOC system is to provide better accountability of classified material and thereby reduce the possibility of loss or accounting error which would result in a costly investigation. Although these unfortunate situations will not be completely eliminated, the COMMANDOC will greatly assist investigation officers in tracking the accountability train of lost or misaccounted documents.

4. Recordkeeping

While the COMMANDOC improves speed and accuracy of accountability, it reduces the size and weight of existing records. One computer diskette can hold the same

information that has previously been maintained in volumes of 8" x 10" x 1/2" logbooks. Many of these logbooks are maintained for years after their creation merely because one (or more) entries are still active in them. The electronic records maintained are more efficient and easier to search than existing manual systems.

The clearance and access information provided to the Department of the Navy Central Adjudication Facility (DONCAF) is entered into the COMMANDOC, thereby providing access control at the user's level. While this may seem like a duplication of effort, it is required in order to provide up-to-date information for the system operator. Processing time for a clearance can take up to six weeks through the DONCAF system. Additionally, interim clearance and access may be granted locally, and immediate updates are required as individuals transfer or have their clearances revoked. When an individual requests a particular document, the COMMANDOC checks his clearance and access levels with those of the document. If they do not match, then the system operator is advised and access is denied.

III. USER REQUIREMENTS FOR COMMANDOC

A. GENERAL

Defining the user's requirements for the database and the applications involves two major goals. The first goal identifies the entities in the user's work environment that he needs to keep track of. These entities are represented as objects, the instances of which will be stored in the database. Examples of such objects in the CMCC environment would include a DOCUMENT, a SAFE, a USER, and an SCP.

The second goal of this phase is to determine the functional components that will be used to update and modify the database. These functional components include update, display, and control mechanisms. These components allow the user to modify data in the database to keep it current as well as retrieve information from it.

This chapter first examines the descriptions of the major objects of the COMMANDOC system and the data elements that comprise them. These verbal descriptions are reinforced by the object diagrams that visually portray the same descriptions. These object diagrams are built after extensive analysis of the existing system and determination of the attributes that comprise each entity. This is accomplished through observation and analysis of a working system, interviews with personnel working with they system, and often through the personal experience of the analyst in the same or similar environment. It is important that the

analyst thoroughly learn all of the mechanisms that are a part of the total system in order to create accurate object models.

The chapter then describes the requirements of this particular application to include the flow of data and the various actions on the individual objects. This discussion and the accompanying diagrams portray the relationships between the various objects and the process through which these objects are transformed. Again, a thorough understanding of the system is essential in order to create an accurate model. The same techniques are used as described in the previous paragraph.

B. DATA REQUIREMENTS: OBJECTS

1. DOCUMENT. The central object of this application is the DOCUMENT object. There are four types of objects: HELD_DOC, TRANSFERRED_DOC, DESTROYED_DOC, and SUB-CUSTODIED_DOC. These types represent four possible phases in the life of a document from the time it is received until it is dropped from the system two years after its destruction or transfer. Each DOCUMENT is uniquely identified by its CONTROL_NUMBER and COPY_NUMBER. Other attributes of particular interest are:

- ORIGINATOR--the name of the organization that created the document.
- ORIGINATOR_SERIAL_#--the original serial number issued by the originator. This number is used for tracking,

reference, and identification purposes by the originator and should not be confused with the control number the receiving command assigns to the document. When the originating command is processing one of its own documents this attribute is left blank.

• SHORT_TITLE--the identifying code provided by various organizations to identify their documents (e.g., APC-1234, OPNAVINST 5510.1H, etc). It is sometimes preferable to conduct an inventory by SHORT_TITLE rather than by LONG_TITLE. Inventories can be printed using either format.

• LONG_TITLE--the complete, formal title of the document. • REGISTERED_MAIL_NUMBER--for documents received by registered mail, this is the number assigned by the post office for the registered mail package. Several documents may come in the same registered mail package and thus have the same REGISTERED_MAIL_NUMBER.

• DECLASSIFICATION_DATE--the date identified on the document when it will be declassified.

• SCI, NATO, and CNWDI are special caveats added to the classification level of a document. These are logical attributes (true or false) which are matched with a USER's clearance and access. That is, a document that includes CNWDI can only be viewed/checked-out to a USER who has CNWDI access.

• SAFE and DRAWER--the number of the safe and drawer in which the document is located. This information is valuable when preparing emergency action inventories for each drawer and safe.

2. DESTROYED_DOC. The DESTROYED_DOC is a subclass of the DOCUMENT object. In addition to inheriting all the attributes of a DOCUMENT, the DESTROYED_DOC also has a DISPOSITION_NUMBER, which identifies the disposition report on which the DESTROYED_DOC was reported as being destroyed, and a DESTRUCTION_DATE.

3. TRANSFERRED_DOC. A TRANSFERRED_DOC is a subclass of the DOCUMENT object. In addition to inheriting all the attributes of a DOCUMENT, the TRANSFERRED_DOC also has a DISPOSITION_NUMBER, which identifies the disposition report on which the TRANSFERRED_ DOC was reported as being transferred; a TRANSFER_ADDRESS, which identifies where the DOCUMENT was sent to; and a TRANSFER_DATE.

4. HELD_DOC. A HELD_DOC is a DOCUMENT that has been checked-out and is being held by an authorized USER. In addition to inheriting all the attributes of a DOCUMENT, the HELD_DOC contains a USER and a CHECK-OUT_DATE.

5. SUB-CUST_DOC. A SUB-CUST_DOC is a DOCUMENT that has been sub-custodied to an SCP. In addition to inheriting all the attributes of a DOCUMENT, the SUB-CUST_DOC also contains an SCP and a SUB-CUST_DATE.

6. USER. The USER object identifies the individuals in the command who are authorized to view or check out material from the CMCC. The collection of these USERS constitutes the command's access list. Any USER may have custody of many HELD_DOCs and may have access to one or more DRAWERs in a safe. Many of the attributes of this object are self-explanatory, but the following require further description.

• CLEARANCE--the current level of security clearance authorized by DONCAF. The codes utilized are the same codes used by MCO P1080.20H (Marine Corps JUMPS/MMSCODESMAN).

• ACCESS--the current level of security classification an individual is authorized to view. While a USER may have received a top secret clearance based on a background investigation, his need-to-know may be limited to the secret level.

• INVESTIGATION_TYPE--the code to indicate the type of security investigation used as the basis for granting a security clearance. The codes used are the same as those listed in MCO P1080.20H.

• AGENCY--the code to indicate the agency that conducted the security investigation used as a basis to grant a clearance. The codes used are the same as those listed in MCO P1080.20H.

• INVESTIGATION_DATE--the date a security investigation was completed and approved.

• NOFORN, SCI, NATO, and CNWDI--special caveats added to the level of access granted to a USER. These are logical fields (true or false) that must match the same fields on a restricted document. That is, a DOCUMENT that has CNWDI (Critical Nuclear Weapons Design Information) restriction placed on it may only be used by a USER with CNWDI access.

• EDD--the USER's estimated date of departure from the command. This is used to estimate when a user will be transferred so that all material checked out can be identified and returned.

• OPID--the operator identification code. This code identifies a person who is authorized to operate the COMMANDOC, such as the CMCC Officer, TSCO, or CMCC Clerk. This field is linked with the operator's password and access level into the COMMANDOC.

7. SCP. An large organization may have one or more SCPs (Secondary Control Points) which maintain accountability for all the documents assigned to a particular section or office. The SCP will of course have many SUB-CUST_DOCs as well as the following traits.

• SCP_CODE--a alphanumeric code to identify the SCP.

• SCP_NAME--a complete name to identify the SCP.

• SCP_CUSTODIAN--a person assigned in writing to be responsible for the accountability of all the DOCUMENTs charged to the SCP.

8. SAFE. A SAFE is a storage container in which a DOCUMENT is stored and contains one or more DRAWERS. A SAFE is identified by its SAFE_NUMBER and SAFE_LOCATION. The ability to identify which DOCUMENTs are assigned to a given SAFE allows an inventory to be prepared for that SAFE. This is helpful when executing an emergency action plan or when the contents of an entire SAFE must be transferred.

9. DRAWER. Each DRAWER must belong to a SAFE. A DRAWER may have one or more USERs and will contain many HELD_DOCs. Each DRAWER is further identified by its DRAWER_NUMBER and OFFICE.

10. PASSWORD. Each person who is authorized to operate the COMMANDOC must be assigned a PASSWORD. Each PASSWORD object contains the following elements.

- OPID--the Operator Identification code is a four digit code that identifies a USER as an authorized operator of the COMMANDOC.
- PASSWORD--the actual password of an authorized operator of the system.
- SYSTEM ACCESS--the level of system access associated with a particular password, and hence, with that operator.
- PW_DATE--the date a PASSWORD was originated. This is used to determine when a PASSWORD must be replaced.

C. APPLICATION REQUIREMENTS

1. Data Flow

The CMCC Officer, TSCO, and clerical personnel assigned to the CMCC are the system operators and will add, update, and delete information contained in the system. They will also query the system as needed and generate various reports. It is common that the CMCC Officer is not concurrently assigned as the TSCO or alternate TSCO, and that the top secret clerk is not concurrently assigned as the CMCC Clerk. In these cases, the CMCC personnel are not permitted to handle the accounting of top secret documents nor are the Top Secret Control personnel authorized to handle the accounting of secret and confidential material. The logical Data Flow Diagram, contained in Figure 4, illustrates the flow of information and is described in detail below.

The primary process of accounting for classified material begins with receipt of classified DOCUMENTs from the originators via authorized couriers or from the post office. All registered and certified mail is opened in the vault and if it contains classified material, it is assigned a CONTROL_NUMBER and is entered into the COMMANDOC. A cover page (OPNAV 5216/10) is filled out and attached to the DOCUMENT. The DOCUMENT is dentified for routing or distribution, and custody is changed as the DOCUMENT moves from USER to USER.

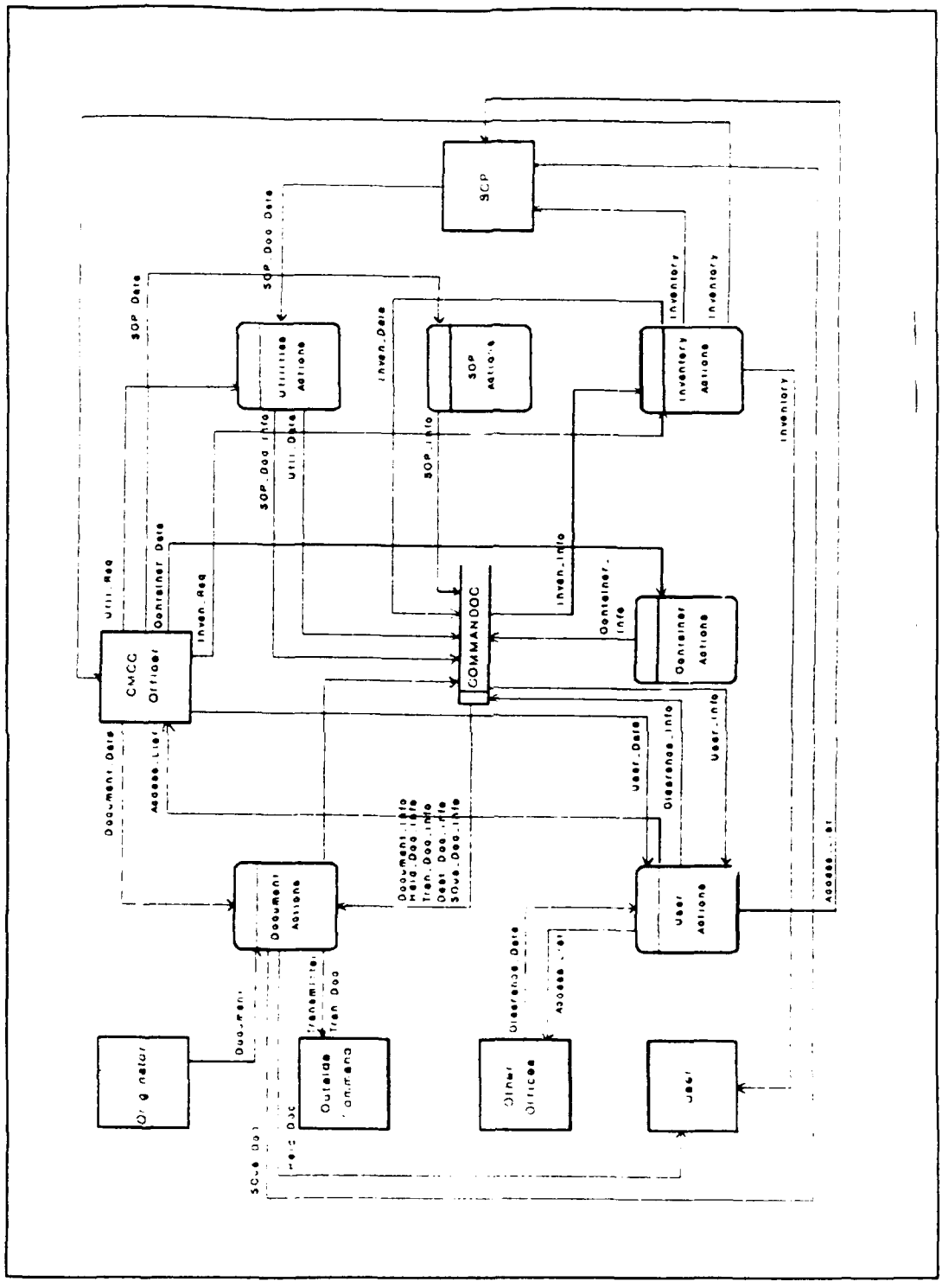


Figure 4. Logical Data Flow Diagram.

Before DOCUMENTs can be subcustodied, SCPs must be established and identified. This is done through formal assignment letters and Physical Security Evaluations of the proposed physical areas and is approved by the Security Manager.

When a USER desires to check out a DOCUMENT, he must properly identify himself and his identity, clearance, and access must be confirmed. The access code will identify the highest classification of classified material the USER can be issued. A request for access is originated by the individual's Officer in Charge and is routed through the organization's Personnel Department for verification and then becomes part of the access list. This list is maintained in the system and is updated as required.

If a DOCUMENT must be transferred to a different organization, a transmittal form is prepared, a disposition number is assigned (prefixed with a "T" for transfer), and the DOCUMENT and transmittal are mailed (or sent by courier) to the new organization. Upon verification by the CMCC Officer, the record of the DOCUMENT is then moved to the TRANSFERRED DOCUMENT file. The transmittal form is signed upon receipt and returned to the sending CMCC.

Similarly, when a DOCUMENT's usefulness is complete, it must be destroyed. Such DOCUMENTs are listed on a destruction report, identified by a disposition number (prefixed with a "D" to indicate destruction), and destroyed

by authorized means. The record of the DOCUMENT is then transferred from the active file to the DESTROYED DOCUMENT file, where it is kept for the required retention period of two years.

Whenever a new CMCC Officer or SCP Custodian is assigned, at least annually (although in practice, most commands require semi-annually), and whenever directed, an inventory of DOCUMENTs must be accomplished. The inventory process will generate a list of all DOCUMENTs assigned to the CMCC, an SCP, or a USER. An inventory must be completed, signed, and returned to the custodian within 15 days, and any discrepancies must be noted. Any material lost or missing must be properly reported and an investigation conducted.

2. Actions

a. Authorization to Conduct Actions

Ultimate responsibility for all transactions rests with the CMCC Officer and is exercised through the SCP Custodians (when SCPs exist). The CMCC Officer, TSCO, SCP Custodians, and clerks are selected for their positions only after a thorough background investigation and personal screening. Only the most conscientious individuals are selected for these positions, and their integrity is normally considered beyond reproach. These individuals will not be considered a source of sabotage to the integrity of the information in the database. Nevertheless, certain

actions are restricted by the system access attached to each operator or the COMMANDOC. For example, the CMCC Custodian is not authorized to enter, modify, transfer, or destroy top secret documents unless he is also designated as the TSCO or alternate TSCO. Figure 5 summarizes these actions by category.

		Documents						Users				SCPs			Safes			Operator			Reports/ Maintenance				
Level	Billet	Enter	Modify	Destroy	Trans	SubCust	CkOutIn	Add	Modify	Delete	List	Add	Modify	Delete	Add	Modify	Delete	Add	Modify	Delete	Update	PsWord	Restore	TrData	RecData
9	SecMngr	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
9	CMCCO/TSCO	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
8	CMCC Cust	S	S	S	S	S	S	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
8	AltCMCCO	S	S	S	S	S	S	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
7	Joint NCOIC	X	X	X	X	X	X	X	X	X	X	X	X	-	X	X	X	-	-	-	X	X	-	X	X
6	NCOIC	S	S	S	S	S	S	X	X	X	X	X	X	-	X	X	X	-	-	-	X	X	-	X	X
5	Joint Clerk	X	X	X	X	X	X	X	X	X	X	-	-	-	X	X	X	-	-	-	X	X	-	X	-
4	CMCC Clerk	S	S	S	S	S	S	X	X	X	X	-	-	-	X	X	X	-	-	-	X	X	-	X	-
3	TCSO	T	T	T	T	T	T	-	-	-	-	-	-	-	-	-	-	-	-	-	T	X	-	-	-
2	TS Clerk	T	T	T	T	-	T	-	-	-	-	-	-	-	-	-	-	-	-	-	T	X	-	-	-
1	SCP Cust	-	P	P	-	P	P	-	-	-	-	-	-	-	-	-	-	-	-	-	P	X	-	-	-
0		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

X = all documents
T = top secret documents only
S = secret and confidential documents only
P = only those documents subcustodied to that SCP
- = no access for any classification

Figure 5. Authorized Access Levels.

b. DOCUMENT Actions

New DOCUMENTs are routinely created as they are received at the CMCC. These new entries are normally made

by the CMCC Clerk (for secret and confidential DOCUMENTS) and TSC Clerk (for top secret DOCUMENTS).

Modification of documents is performed at the direction of the CMCC Officer whenever errors are discovered, and routinely by the Clerk(s) when routine transactions (such as change of location, SCP, or USER) occur. Key fields (CONTROL NUMBER and COPY NUMBER) may not be modified. Again, only TSC personnel are authorized to modify top secret documents, and TSC personnel are not authorized to modify non-top secret DOCUMENTs unless they are jointly assigned to both positions.

Destruction or transfer of DOCUMENTs is directed by the CMCC Officer, normally with the recommendation of the staff officer having cognizance over the subject matter of the DOCUMENT. The clerk prepares a destruction or transaction report, but the CMCC Officer must sign the printed report and is thereby kept informed of the transactions that are occurring within his account. Again, only TSC personnel are authorized to modify top secret documents and Top Secret Control personnel are not authorized to modify non-top secret DOCUMENTs unless they are jointly assigned to both positions.

c. USER Actions

A new USER may be added to the COMMANDOC by the CMCC Clerk based upon locally established procedures (usually a form letter signed by the Security Manager).

This administrative action is normally a routine entry made by the CMCC Clerk.

Modifications to USERs will normally be directed by the CMCC Custodian and the clerical action taken by the CMCC Clerk.

Deletions of USER records will be handled in the same manner as modifications, except that USERs are routinely dropped during the process of checking-out of the organization. The USER object will not actually be deleted but is removed from an active status. The record remains inactive for the required retention period (two years) and is then purged from the system. This is to permit a complete record of information should it become necessary to conduct an investigation at some later time.

d. SCP Actions

An SCP may be added and modified by either the CMCC Custodian or CMCC NCOIC. An SCP will only be deleted by the CMCC Custodian. Adding or modifying an SCP is an infrequent event and is usually administrative in nature (i.e., changing its name or the name of the SCP Custodian). Nonetheless, it should be completed at a level higher than the CMCC Clerk. Deleting an SCP is a more significant step and should involve the direct participation of the CMCC Custodian.

e. SAFE and DRAWER Actions

A DRAWER must belong to an already established SAFE. Actions to both SAFEs and DRAWERs are routine matters and can be accomplished by the CMCC Clerk. While these entities are not critical to the COMMANDOC system nor to the DOCUMENTs they contain, they provide a very useful administrative purpose. The COMMANDOC system permits an inventory to be prepared by SAFE/DRAWER. Such inventories are useful for emergency action plans which call for the transfer or destruction of large quantities of classified DOCUMENTs. An immediate, up to date inventory or each DRAWER will assist in the administrative record keeping of transferring or destroying an entire container.

IV. COMMANDOC SYSTEM DESIGN

A. LOGICAL DATABASE DESIGN

The process of designing a logical database consists of drawing together the concepts presented in chapters II and III in order to produce the master plan for the structure of the actual database. This physical design of the database is specific to a particular application while the logical design is a generic one.

Logical database design involves transforming objects inot relations and their associated relationships. The basis for performing logical database design is the concept of binary relationship. A binary relationship is a relationship between two record types.

In the example shown in Figure 6, the object of a SAFE and a DOCUMENT on the left are transformed into the

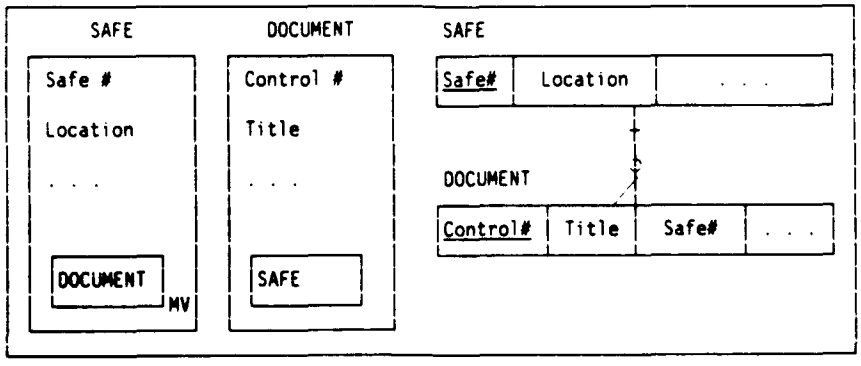


Figure 6. Transformation of Objects to a Relation.

relations and relationship on the right. The SAFE object is identified by its Safe#, Location, and other fields. The

DOCUMENT within the box indicates the presence of another object within this first object. The MV indicates multiple values of this second object. In plain terms, this diagram reads: "A SAFE has a safe#, a location, and contains multiple DOCUMENTS." The DOCUMENT object can be described in a similar manner, but note the absence of the MV status of the SAFE object within DOCUMENT. This indicates one (and only one) instance of a safe is related to each DOCUMENT. Again in plain terms: "A DOCUMENT has a Control#, a Title, and is stored in a SAFE." Note that any instance of a DOCUMENT can only be located in one SAFE at any time.

The second set of diagrams shows the relationship of these two objects. The vertical line indicates a relationship. The shorter horizontal bar near the upper end of the relationship line indicates a mandatory relationship--each DOCUMENT must have a SAFE. The small circle at the lower end of the line indicates a minimal relationship is allowed, that is, a safe could be empty and not possess any DOCUMENTs. If the line had neither a bar nor a circle it would indicate that a "one-to-one" relationship existed--for each SAFE there would be one (and only one) DOCUMENT. The forked end of the relation line indicates a "many" relationship while a single end represents a "one" relationship. In plain terms, this diagram reads: "One SAFE (consisting of a Safe# and a Location) contains many DOCUMENTs (consisting of a Control#, Title, and Safe#)."

Another way of describing this relationship is to think of the SAFE relation as the parent and the DOCUMENT as the child. Each parent may have many children, but a child can only have one parent.

Two additional items must be explained pertaining to the second set of diagrams. Notice that "Control#" in DOCUMENT and "Safe#" in SAFE are underlined. This indicates that this attribute is a key field, that is, an attribute that uniquely identifies each instance of the relation. In this case, each document has a different Document# and each safe has a different Safe#. Also note that Safe# is contained in both relations, although not identified as a key field in the DOCUMENT object. In order to establish a relationship between the two relations, there must be a common link between them. This field is referred to as a foreign key. In this example, all DOCUMENTs with Safe# = X are related to (i.e., are stored in) SAFE X.

Figure 7 contains the object diagrams for the objects contained within COMMANDOC. Object definitions with attributes, types, and lengths, and the domain definitions with attributes, masks, and descriptions are contained in Appendices B and C. Figure 8 displays the relation diagram which shows the relations, attributes, and relationships of the system.

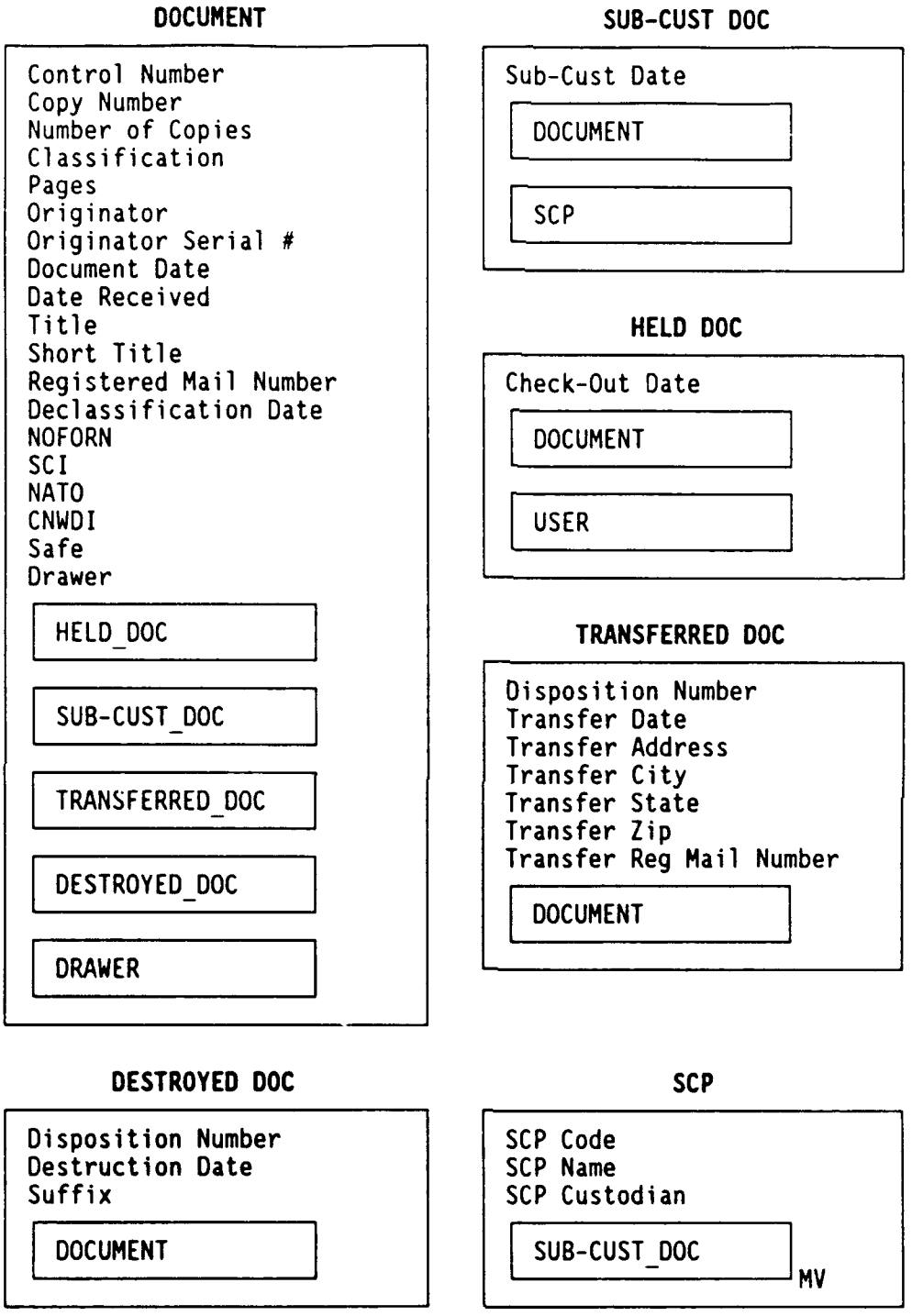


Figure 7. Object Diagrams.

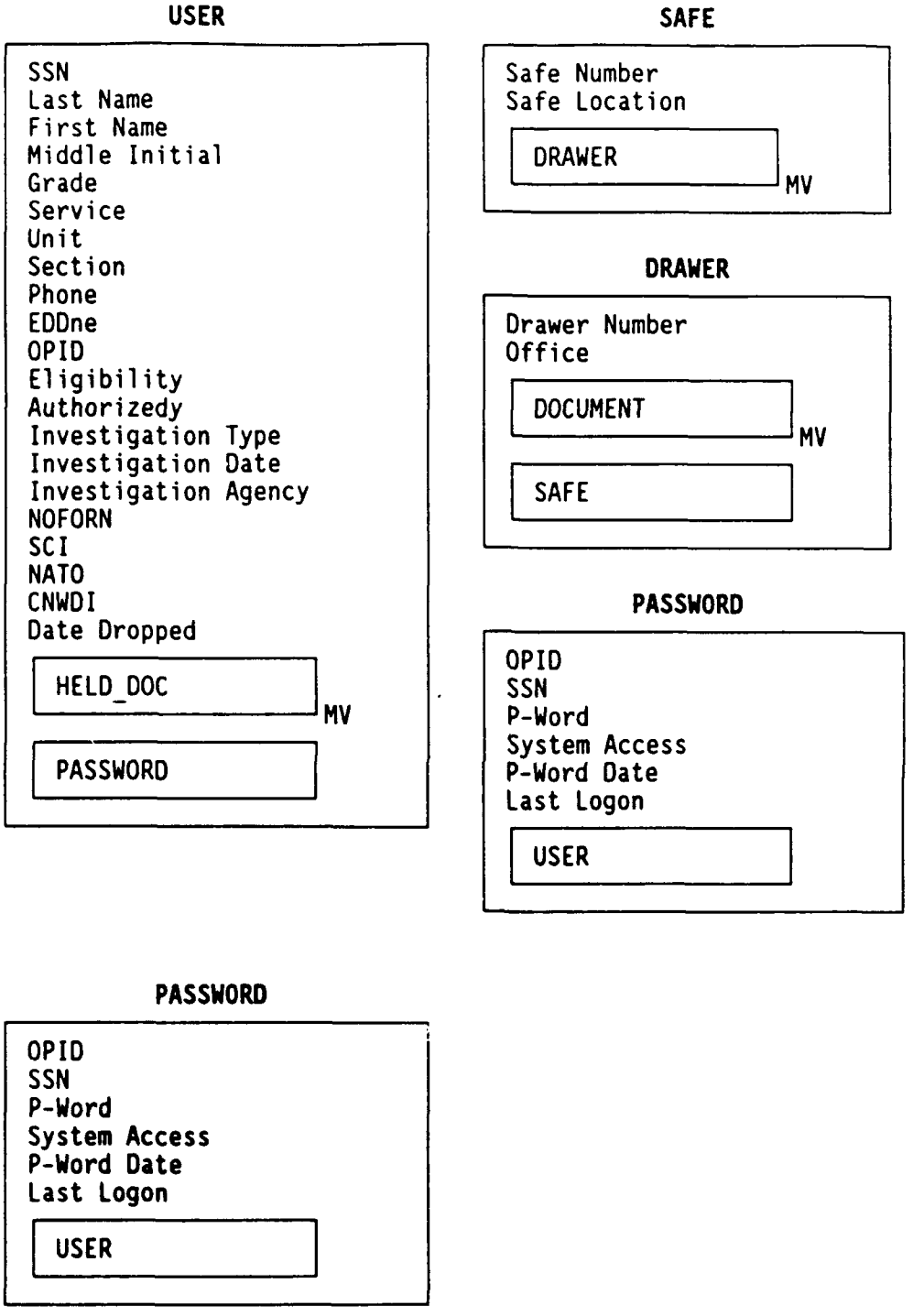


Figure 7 (cont). Object Diagrams.

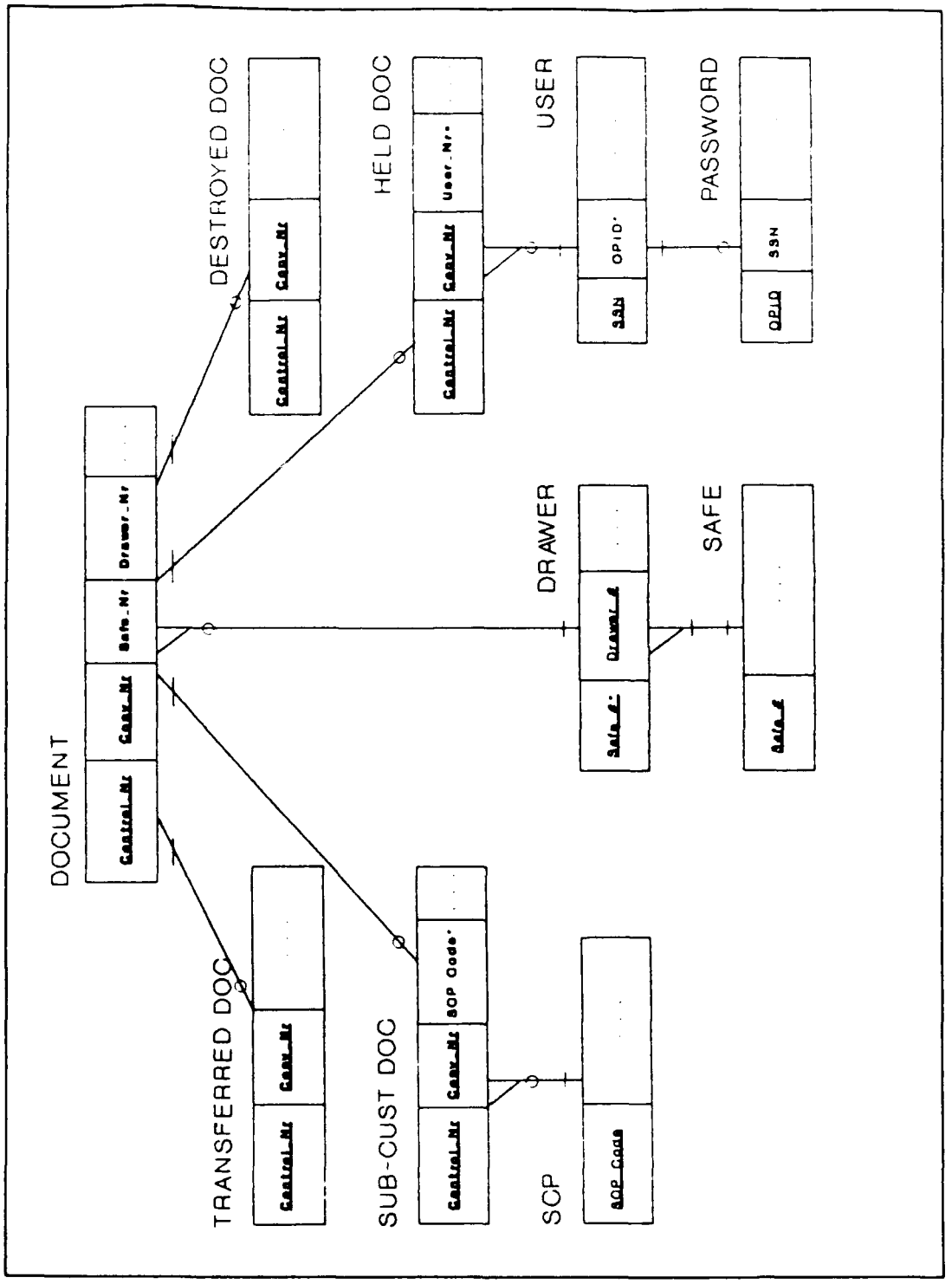


Figure 8. Relation Diagram.

For each controlled DOCUMENT, multiple copies may be produced and must be tracked in the COMMANDOC. It therefore requires a combination key (Control Number, Copy Number) to uniquely identify a tuple in the DOCUMENT relation. The four document types (Held, Sub-Custodied, Transferred, and Destroyed) have the same key fields. Each document type must be associated with a DOCUMENT but a DOCUMENT is associated with only one of the document types. This unique relationship, where objects are significantly but not completely similar, is referred to as a generalization object and they are depicted in the accompanying diagrams by a filled triangle in the upper left hand corner of the object box.

A Secondary Control Point (SCP) may have many DOCUMENTs sub-custodied to it, but documents can only be sub-custodied to an SCP. Secondary Control Point Code is the key to the SCP relation. It is also a foreign key in the SUB-CUST DOC relation.

Any DOCUMENT held must be kept in a DRAWER which must belong to a SAFE. A SAFE will have at least one DRAWER. A DRAWER can hold many HELD DOCs. Safes are identified by a unique number, and that key field makes up part of the composite key (i.e., Safe #, Drawer #) in the DRAWER relation.

A USER may check out many DOCUMENTs, and any HELD DOC can be loaned to a single USER. A USER may have a PASSWORD

assigned to him and a PASSWORD must have a USER associated with it.

B. APPLICATION DESIGN

1. Menu Hierarchy

The COMMANDOC is a menu driven application intended to require little or no previous computer experience. The typical clerk and custodian in a CMCC office have little computer experience and often only moderate typing skills. The CMCC Officer is normally assigned as an additional duty to an already busy schedule. The COMMANDOC is designed to require the involvement of the CMCC Officer to ensure his active participation in the account. At the same time, it automates and eases his responsibilities by providing the information needed to adroitly manage the account in an informative and easy to use manner.

The menu hierarchy presented in Figures 9a-c is developed from the Object/Action perspective. The Main Menu has choices providing access to Document Actions, Secondary Control Point Actions, User Actions, Safe/Drawer Actions, Inventories, and various Utility Actions. Selections from subordinate menus may call other actions (grouped appropriately) or action screens. Figure 10 is an example of a data entry screen. Items with a major block heading but no subordinate entries take information from the system operator with a date entry screen. There are a variety of data entry screens and many provide a dialog between the

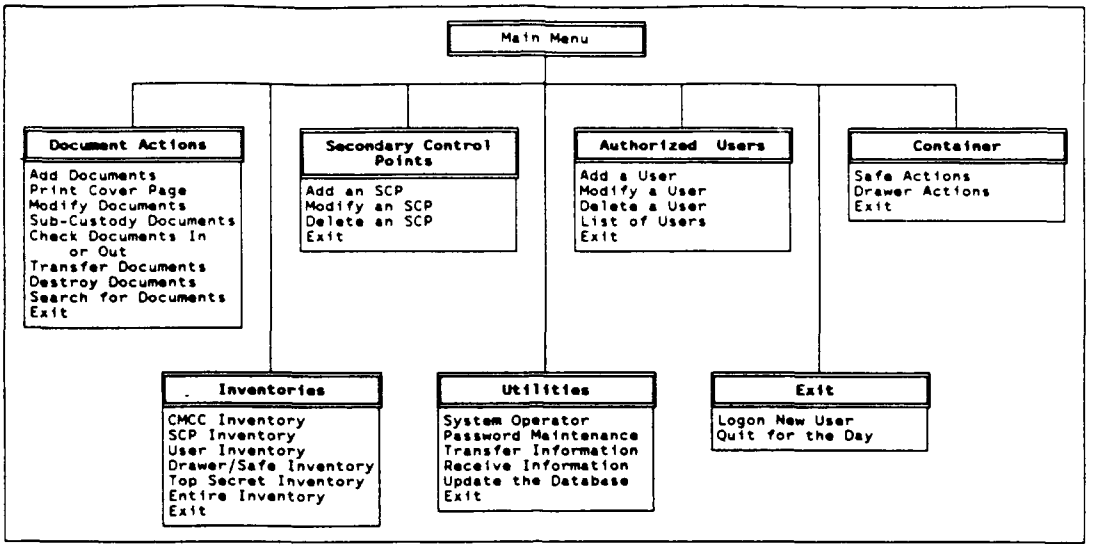


Figure 9a. Main Menu Hierarchy.

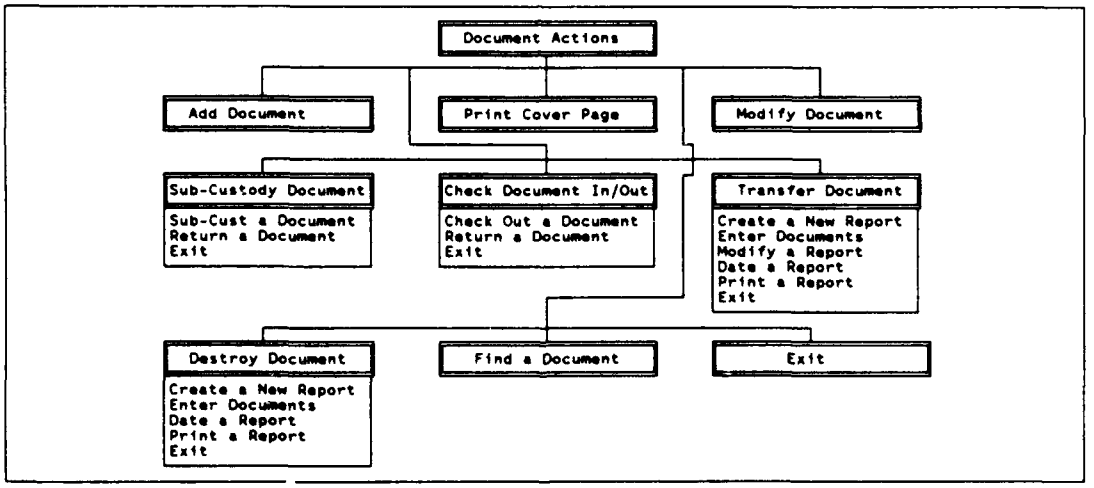


Figure 9b. Document Action Menu Hierarchy.

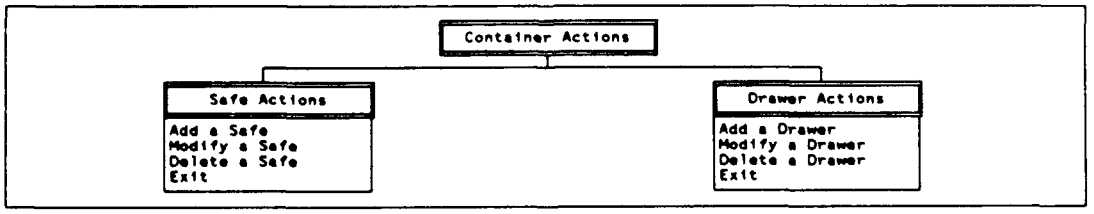


Figure 9c. Container Action Menu Hierarchy.

COMMANDOC and the system operator. For example, after data is entered into the data entry screen the system will ask if the information is correct or provide an error notification if incorrect data was provided.

```
                          DOCUMENT ENTRY SCREEN

Control# Copy   Of Class NOFORN SCI NATO CNWDI Date Recd #Pages Reg Mail #
91-00104    1    1   S      N    N    N    N    28APR91     35  R-45837461

Originator                                Orig Ser #   Doc Date  Declass
CG, 1ST MARDIV                            91-S-09475   09MAR91   OADR

Subject                                                  Location
APPENDIX B TO CG 1STMARDIV OPLAN 91-123                  Safe      Drawer
                                                         S305        2

Short Title
APPX B OPLAN 91-123

                      Correct information? (Y/N)
```

Figure 10. Sample Date Entry Screen.

2. Reports

The COMMANDOC will produce a variety of reports, both for the actual functioning of the system as well as for advising the CMCC Officer of the status of the account.

•LOGBOOK: The COMMANDOC automates this process by extracting all active documents sorted by user and SCP codes. The COMMANDOC also retains destroyed and transferred records for their required periods. By doing this, the CMCC is no longer required to keep bulky logbooks on file for

(conceivably) ten or more years because one or more entries in the book is still active.

•COVER PAGE: The COMMANDOC is designed to print the required data on the standard OPNAV 5216/10 form. Not only does this reduce the time required to complete the form, it also improves the form's accuracy. One copy of the form is maintained in the CMCC and provides two important functions: (a) it acts as a manual backup system and (b) provides a source of signatures to confirm subcustody or check-out of a document. This first function is particularly useful for the expeditionary nature of Marine Corps forces that may be called to operational commitments that may not afford the benefit of using a computer. The second function enhances the familiar chain of custody and verifies the action taken on a document.

•INVENTORY: The COMMANDOC automates this process and provides a printed inventory upon request, sorted by entire CMCC, SCP, or individual user, and may be generated for secret and confidential documents or for top secret documents only. Inventories must be certified by the responsible officer, returned to the CMCC, and maintained for two years (five years for Top Secret material).

•DESTRUCTION REPORTS: The COMMANDOC automatically creates destruction reports based upon the entry of the document control number. The clerk also enters the date of the destruction and the system generates the

next sequential report number. The destroyed documents are maintained in a destroyed status and are automatically purged from the system after the requisite retention period (depending upon classification). In the event a destruction is completed by an SCP, a floppy disk containing the report information can be transferred to update the CMCC's master file. Refer to Section 6 of Appendix D for further details on this process.

•TRANSFER REPORTS: The COMMANDOC automatically creates transfer reports. The clerk enters the control numbers of the documents to be transferred, the date of the transfer, and the command to which the documents are being sent. The system generates the next transaction number, assigns it to the documents identified for transfer, and prepares the report. The transferred documents are maintained in a transferred status and are automatically purged from the system after the requisite retention period (depending upon classification). Since documents can only be transferred from the CMCC, there are no provisions for a disk update of transferred documents from an SCP.

•SUBJECT/TITLE SEARCH: The COMMANDOC utilized the power of the computer to simplify this task. The clerk enters the keyword of the material that the user needs and the system automatically searches the database to find all references to that keyword within the first 45 characters of the title, including documents maintained in the destroyed

or transferred status. This feature supports the use of the wildcard characters "%" and "*". Of course, if the document was transferred/ destroyed beyond the two year filing period, there will be no record of it.

•REGISTERED MAIL SEARCH: The COMMANDOC can accomplish this type of search in seconds. The clerk enters the registered mail number and the system searches the database for a match. All documents (active, transferred, or destroyed) that are associated with that registered mail number are then displayed and their status verified. As with the title search, the use of wildcards is supported.

•EMERGENCY ACTION PLAN INVENTORIES: The COMMANDOC supports the Emergency Action Plan (EAP) by providing the ability to create inventories of each drawer of each safe. This is helpful because material is usually stored segregated by classification level and is could be conveniently "packaged" by drawer. An EAP inventory could be produced by each drawer and easily used as a transfer inventory or destruction inventory during a period when extra time for these administrative responsibilities may not exist.

•USAGE REPORT: Existing systems have no equivalent of the usage report that the COMMANDOC can provide. This report is provided on a weekly basis to the CMCC Custodian to inform him of the time each operator of the system has logged on. This information will help

identify possible tampering with the system. For example, the CMCC Custodian might question why a particular operator was using the system from 0100 to 0130 on a Saturday night. While no requirement exists for such a report to be maintained within the security of classified material, it does add an additional of depth to the command's security program.

3. Passwords

In order to ensure the integrity of the database, the COMMANDOC utilizes a password system that limits an operator's access to perform only those functions assigned to his billet. Figure 5 previously displayed the functions that are authorized by billet. The procedures utilized by the COMMANDOC follow the guidelines set forth in the Department of Defense Password Management Guideline, (CSC-STD-002-85)--the password system provides for personal identification, authentication, password privacy, and auditing. The passwords utilized in the COMMANDOC must be renewed at least every six months and the minimum eight character size presents sufficient length to ensure resistance against being "guessed" within its useable lifetime. As with any password system, however, the security provided is lessened when the user selects easily guessed passwords like name combinations, birthdates, social security numbers, etc.

An added level of security is provided when the computer the COMMANDOC is operated on is located within a security area (vault or strongroom). This will keep the system free from unscrupulous attempts to damage the data files. That is to say, an additional "password" is in fact the classified combination to the vault or strongroom known only to the CMCC Officer and clerks.

When a USER is authorized to be a system operator by the CMCC Officer, the a four-digit OPID (Operator Identification) code is generated by the system and a PASSWORD is generated for that new OPID. The original PASSWORD will be "PASSWORD" and must immediately be changed by the new system operator. A PASSWORD has a date it was created (P-Word Date) and must be changed at least every six months. Just like a combination to a lock, however, a PASSWORD must also be changed whenever it has been compromised.

4. File Portability

a. Distributing the System

The COMMANDOC is designed to be freely distributed and utilized as an administrative assistant to all holders of classified material. Accordingly, a slightly modified copy of the system is provided that can be copied from the CMCC to an SCP within a command. In this manner, each office within the command will utilize the same record keeping process for accounting for its classified material.

b. Downloading the Database

In such an environment where the SCPs of a command also utilize the COMMANDOC, the system will create a copy of each SCPs documents and users database onto floppy disks for transfer to a remote location. This will ensure that the SCP works only with documents created by the master system and will not corrupt the integrity of the system.

c. Uploading Information

Just as the SCP must receive information from the master database, so too the master database must receive certain information from the local SCPs. The most common reason for a data upload will be for reporting destruction of classified documents. The SCPs are responsible for their own destruction of classified material and will have to relay this information to the master database at the CMCC.

In existing systems, the SCP forwards copies of destruction reports to the CMCC where their corresponding entries are entered into the logbook and then lined out with a highlighter. The COMMANDOC allows for the SCP to send the destruction report data on diskette to the CMCC where the data can be uploaded and the records in the master database updated accordingly. As stated above, destroyed records are maintained in the system for the designated period.

5. Protection of Files

a. It is imperative that the data files of any DBMS be backed up routinely and that a system exists to rebuild the database in the event of any form of disaster. The manager of a system who avoids this principle is liable for the resulting losses that will occur when (not if) a problem arises that requires the database to be rebuilt. The COMMANDOC system automatically creates a backup every time the system is properly closed down. Section 8 of Appendix D covers this procedure in detail.

b. The security of a system will always be challenged by unscrupulous individuals who have access to it. This may occur because the operator is challenged by the design of the security features or may be an intentional act aimed at destroying, damaging, or manipulating data for mischievous or criminal reasons. The COMMANDOC system does not encrypt the entire database every time it is saved. Thus, it is vulnerable to malicious tampering or editing by various commercial products outside of the COMMANDOC shell. This is not considered to be a major flaw, however, because of the trusted environment that COMMANDOC is operated in. Each operator of the system is carefully screened for their integrity and honesty prior to being assigned to the CMCC. Actions of a malicious nature by an untrustworthy individual should be viewed more as a deficiency of managerial oversight rather than of the COMMANDOC system itself.

V. CONCLUSIONS

A. LESSONS LEARNED

The development of the COMMANDOC system answers the basic thesis question that a DBMS can be utilized to effectively track the administrative processing of classified documents in a CMCC. The principles involved would apply to any system of controlled items, classified or unclassified, where strict accountability is required. Examples might include an armory, a supply point, or a motor pool.

The specific lessons learned from this thesis pertain to the actual building of the DBMS. The first iteration of the system was a prototype written in dBASE III Plus that maintained all documents in a single flat file. No automatic provisions existed for purging old and expired records and the housekeeping of the system depended on level of the user's computer experience. While the daily operation was designed for the non-technical user, the usefulness of the system would diminish significantly after its inventor was transferred from the command. This is a problem that plagues many locally invented programs and was a forethought in designing COMMANDOC--develop a system that would automatically purge itself of old records and perform routine housekeeping matters with little, if any, user assistance.

The second iteration of the system began integrating databases and developed a relational database model. A small test version of the system was built using dBASE IV, but the response time was incredibly slow. The decision was made that such slow response time would deter general users from utilizing the system and a faster software package was sought. This problem was resolved with another test version that was built in FoxBase III. The speed difference between dBASE IV and FoxBase III was significant and obvious to any observer.

Review of product availability suggested yet another alternative to build the final application--FoxPro 1.02. But at that time, continual reference was being made to an upgrade--FoxPro 2.0. An additional feature that FoxPro 2.0 would provide that the previous software packages did not possess was the ability to generate executable files (.EXE files) from the FoxPro source code. This capability is available through additional products such as Clipper, but subtle differences in programming techniques and command structure could prevent the COMMANDOC system from compiling properly. This additional feature of FoxPro would make it possible to develop the COMMANDOC system, compile it to an .EXE file, and then distribute it freely without incurring the cost of buying a software package for every PC that would run the program.

B. THE FUTURE OF COMMANDOC

While COMMANDOC should prove to be satisfactory for the operation of most CMCCs, there are some possible extensions that could be carried into future versions. For example, in a large CMCC operation controlling thousands of documents, and possibly hundreds on a daily basis, some improvement could be made by utilizing bar codes for control numbers and bar code scanners to conduct inventories. Such a systems would have a much higher cost than the system provided by this paper; scanners and bar code generators are not normally found in an average CMCC or battalion administrative office.

As mentioned at the beginning of this thesis, COMMANDOC is designed to be an unclassified tool for managing the accountability matters of classified documents. The need may also exist for a similar accounting tool to assist managers in the more tightly controlled realm of sensitive compartmented information. While the principles used in COMMANDOC could be modified for use in this environment, special attention would have to be given to many additional security issues including the TEMPEST hazard (electromagnetic emanations that could compromise the classified material entered into the system) and additional physical protective measures for the classified computer itself. Further discussion of these issues are beyond the scope of this paper.

C. CONCLUSIONS

Physical security is composed of many elements. Maintaining accurate accountability of classified documents will not present the malicious compromise or theft of this material, but will reduce the administrative burden that is associated with controlling anything of value. Such a system will, however, reduce the likelihood of a document being accounted for as lost when it has been destroyed or transferred.

APPENDIX A

GLOSSARY OF ABBREVIATIONS

ACMCCO - Assistant Classified Material Control Officer
BAS - Basic Allowance for Subsistence
BAQ - Basic Allowance for Quarters
Capt -Captain (USMC)
CMCC - Classified Material Control Center
CMCCO - Classified Material Control Officer
CNWDI - Critical Nuclear Weapons Design Information
CODESMAN - Codes Manual (USMC)
COMRATS - Commuted Rations
COMSEC - Communication Security
Cpl - Corporal
DBMS - Data Base Management System
DONCAF - Department of the Navy Central Adjudication Facility
EAP - Emergency Action Plan
EDD- Estimated Date of Departure
JUMPS/MMS - Joint Uniform Military Pay System/Manpower Management System (USMC system)
LCpl - Lance Corporal
MOS - Military Occupational Specialty (USMC designation)
NATO - North Atlantic Treaty Organization
NCOIC - NonCommissioned Officer In Charge
NOFORN - No Foreign dissemination
OPID - Operator Identification
PC - Personal Computer
Sgt - Sergeant
SSgt - Staff Sergeant
TS - Top Secret
TSC - Top Secret Control
TSC Clear - Top Secret Control Clerk
TSCO - Top Secret Control Officer
T/O - Table of Organization
SCI - Sensitive Compartmented Information
SCP - Secondary Control Point
USMC - United States Marine Corps

1stLt - First Lieutenant (USMC)

APPENDIX B

OBJECT DEFINITIONS

DOCUMENT Object

Control Number;	Document Number
Copy Number;	Number
Number of Copies;	Number
Classification;	Class
Pages;	Number
Originator;	Command
Originator Serial Number;	Serial Number
Document Date;	Date
Date Received;	Date
Title;	Title
Short Title;	Short Title
Registered Mail Number;	Mail Number
Declassification Date;	Date
NOFORN;	Special Access
SCI;	Special Access
NATO;	Special Access
CNWDI;	Special Access
Safe;	Number
Drawer;	Number
HELD DOC;	HELD DOC object
SUB-CUST DOC;	SUB-CUST DOC object
TRANSFERRED DOC;	TRANSFERRED DOC object
DESTROYED DOC;	DESTROYED DOC object
DRAWER;	DRAWER object

HELD DOC Object

Check-Out Date;	Date
DOCUMENT;	DOCUMENT object
USER;	USER object; SUBSET [SSN]

SUB-CUST DOC Object

Sub-Cust Date;	Date
DOCUMENT;	DOCUMENT object
SCP;	SCP object; SUBSET [SCP
Code]	

TRANSFERRED DOC Object

Disposition Number;	Disposition Number
Transfer Date;	Date
Transfer Command;	Command
Transfer Address;	Address
Transfer City;	City
Transfer State;	State
Transfer Zip;	Zip
Transfer Reg Mail;	Mail Number
DOCUMENT;	DOCUMENT object

DESTROYED DOC Object

Disposition Number;	Disposition Number
Destruction Date;	Date
Suffix;	Suffix
DOCUMENT;	DOCUMENT object

USER Object

SSN;	SSN
Last Name;	Name
First Name;	Name
Middle Initial;	Name
Grade;	Grade
Service;	Service
Unit;	Office
Section;	Section
Phone;	Phone Number
EDD;	Date
OPID;	Operator ID number
Eligibility;	Class
Authorized;	Class
Investigation Type;	Investigation Type
Investigation Agency;	Agency
Investigation Date;	Date
NOFORN;	Special Access
SCI;	Special Access
NATO;	Special Access
CNWDI;	Special Access
Date Dropped;	Date
HELD DOC;	HELD DOC object; MV; SUBSET [Control Number, Copy Number]
PASSWORD;	PASSWORD object

SCP Object

SCP Code;	SCP Code
SCP Name;	SCP Name
SCP Custodian Last Name;	Name
SCP Custodian First Name;	Name
SCP Custodian Middle Initial;	Name
SCP Custodian Grade;	Grade
SUB-CUST DOC;	SUB-CUST DOC object; MV

SAFE Object

Safe Number;	Number
Safe Location;	Location
DRAWER;	DRAWER object; MV

DRAWER Object

Drawer Number;	Number
Office;	Office
DOCUMENT;	DOCUMENT object; MV
SAFE;	SAFE object

PASSWORD Object

Operator ID;	OPID
P-Word;	Password
P-Word;	Date
System Access;	System Access
Last Logon;	Date-Time
USER;	USER object

APPENDIX C

DOMAIN DEFINITIONS

ADDRESS
    Text 30
    Address information of an organization or command

CITY
    Text 25
    City location of an organization or command

CLASS
    Text 1, mask X
        where X is the level of classification of a document. The alpha-numeric code is taken from the JUMPS/MMSCODESMAN (par 111.3). Usually, only codes C (confidential), S (secret), and T (top secret) are used.
    The classification of a DOCUMENT or the access or clearance level of a USER

COMMAND
    Text 35
    Name of an organization or command

CONTROL NUMBER
    Text 8, mask YY-99999
        where YY is the last two digits of the calendar year and 99999 is the next sequential number for a document
    The control number for a given document

DATE
    Text 7, mask DDMMMYY
        where DD is day, MMM is three letter month code, and YY is the last two digits of the calendar year
    Used for all references to a date

DATE-TIME
    Text, mask DDMMMYY-HHNN
        where DD is day, MMM is three letter month code, YY is the last two digits of the calendar year, HH is the hour, and NN is the minute as taken from the computer system
    Used to record and display the last date and time a given PASSWORD was used to logon to the system

DISPOSITION NUMBER
Text 9, mask XYY-99999
where X is the type of transaction (T for transfer or D for destruction), YY is the last two digits of the calendar year, and 99999 is the sequential number
Identifies the transaction that reports the transfer or destruction of classified documents

GRADE
Text 6, mask XXXXXX
where XXXXXX is an authorized grade abbreviation (for military personnel) or government employee designator (for civilian personnel)
Identifies the military or government grade of a user

INVESTIGATION AGENCY
Text 1

Identifies the agency conducting the security clearance investigation for a user. Utilizes the alpha-numeric codes found in the JUMPS/MMSCODESMAN (par 1118.5)

INVESTIGATION TYPE
Text 1
Identifies the type of security investigation completed for a user. Utilizes the alpha-numeric codes found in the JUMPS/MMSCODESMAN (par 1118.4)

LOCATION
Text 10
Describes a physical location such as a building, room, etc.

MAIL NUMBER
Text 10
The registered mail receipt number the transmits a package containing classified documents

NAME
Text 15
Last name, first name, or middle initial of an individual

NUMBER
Text 4
Copy number, number of copies, safe, drawer, number of pages, etc.
Used generically whenever a number is required to describe an entity but is used as a character vice numeric type

OFFICE
    Text 6
    General format to describe a office, unit, or other location

OPID
    Text 4
    The operator identification number used to identify the individual actually operating the COMMANDOC

PASSWORD
    Text 8
    The encrypted password of an operator of the COMMANDOC

PHONE NUMBER
    Text 13, mask (999)999-9999
        where (999) is either the three-digit area code of a commercial phone number (enclosed in parenthesis) or "(AV)" for an AUTOVON number, and 999-9999 is the standard seven-digit phone number. Foreign telephone numbers may utilize the entire 13 digit length as necessary.
    Identifies the phone number of a USER

SCP CODE
    Text 1
    A locally issued, alpha-numeric code to identify a Secondary Control Point

SCP NAME
    Text 15
    An plain English descriptive title for a Secondary Control Point

SECTION
    Text 4
    Local code or abbreviation for a section, division, department, company, squad, etc.

SERIAL NUMBER
    Text 10
    Original serial number issued by the originator of a document

SERVICE
    Text 6
    Identifies the branch of service (United States or foreign) of a user (i.e., USMC, USN, JMSDF, etc.)

SHORT TITLE
    Text 25
    Short title for inventory control of NWPL, CNWDI, technical manuals, directives or other materials that use an identifier other than a plain English title

SPECIAL ACCESS
    Logical
    Identifies as true/false or yes/no if a document or individual requires or possesses special access authorization for SCI, NATO, or CNWDI material

SSN
    Text 9
    Standard social security number for a user

STATE
    Text 2
    Standard two-digit state abbreviation code

SUFFIX
    Text 1
    The code of the SCP or CMCC that has taken action on a document or report

SYSTEM ACCESS
    Text 1
    Access level code for an operator of the COMMANDOC

TIME
    Numeric 4, mask HHMM
        where HH is hours (using a 24-hour clock) and MM is minutes
    The time setting taken from the computer's operating system

TITLE
    Text 90
    The plain-English title of a document, abbreviated as necessary to 90 characters

ZIP
    Text 10, mask 99999-9999
        where 99999 is the basic five-digit zip code and 9999 is the zip + 4 code for an address
    The standard zip code (+4) for an address

APPENDIX D. USER'S MANUAL

GENERAL INFORMATION

INTRODUCTION

1. General. The **COM**mand **MAN**agement of Classified **DOC**uments (COMMANDOC) system is designed to allow a new user to effectively control a system of classified documents with a minimal amount of training. The system operator is guided through the various operations by a system of menus. Choices to the menus may be made by selection of a number or a letter as indicated on each menu. A dialog line at the bottom of the screen guides the operator through the various actions. In short, the operator simply selects an action and then completes the information on the screen. The COMMANDOC system requires the operator to backup the database at the end of each session and performs a variety of logic checks on the data that is entered. Each operator is assigned a password and a level of access corresponding to his position. Routine audit reports provide the supervisor with a history of who has been using the system and for how long.

2. Hardware Requirements. The COMMANDOC system is designed to run on an IBM-compatible personal computer running MS-DOS 3.X or higher with a hard disk drive (20 MB recommended) and one 5 1/2" floppy disk drive. An AT-class machine with an 80286 processor is preferred over an 8088 or 8086 processor.

A dot matrix printer is required in order to produce the required reports and document cover pages.

3. Software Requirements. The COMMANDOC system was designed to be freely distributed without the need for a parent program such as dBase, FoxBase, FoxPro, or similar commercial product. The program is distributed on a 5 1/2" low density floppy disk. The PC that the system will be running on must have MS-DOS version 3.X or higher and the DOS subdirectory must be in the path command in order for COMMANDOC to run properly. A files and buffers statement must appear in the CONFIG.SYS file. FILES=60 and BUFFERS=20 is the recommended setting (based on a 80286 machine running at 8 MHz). While experienced users may experiment to find their optimum settings, the files statement must remain at 60 because of the large number of interactive files the COMMANDOC maintains.

INSTALLATION

1. The COMMANDOC system is distributed on one 5 1/2" floppy diskette. The following steps describe the basic installation process. The user should review any comments in the "README.TXT" file before installing the program. A copy of this user's manual is distributed with the program in the file "DOCUMENT.TXT."

a. Insert the distribution disk into drive A and type "A:INSTALL <┘".

b. Answer the questions that appear on the screen. The batch file will create a new subdirectory and install the necessary files into the subdirectory on the hard disk. This process will ask for the name and address of the command. The accuracy of this information is important because it will be the mailing address on various reports that COMMANDOC prepares.

c. Remove the diskette from drive A and store it in a safe place--it may be needed at a later time to reinstall the program.

d. To commence using the system, type "COMMANDO" at the C: prompt. Note that the name COMMANDOC is truncated after the eighth character.

LOGGING ON THE FIRST TIME

1. The first time the COMMANDOC system is started it should be entered by the CMCC Officer. The system has a primary operator entered with a user name of "CUSTODIAN," the password of "PASSWORD," and access level "8." Upon entering the system for the first time, the CMCC Officer must enter himself as a new user, set the appropriate level of access (see Figure D-1), and then delete the user "CUSTODIAN." If this is not done, then anyone can enter the system and grant themselves access level beyond that which is authorized.

2. Whenever an operator logs on, COMMANDOC will display a warning screen which sets forth the terms of use of the

		Documents						Users				SCPs			Safes			Operator			Reports/ Maintenance				
Level	Billet	Enter	Modify	Delete	Transact	Sub Cust	Ck Out	Add	Modify	Delete	Lists	Add	Modify	Delete	Add	Modify	Delete	Add	Modify	Delete	Update	Psswrd	Reset	Trans	Rec Data
9	SecMngr	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
9	CMCCO/TSCO	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
8	CMCC Cust	S	S	S	S	S	S	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
8	AltCMCCO	S	S	S	S	S	S	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
7	Joint NCOIC	X	X	X	X	X	X	X	X	X	X	X	X	-	X	X	X	-	-	-	X	X	-	X	X
6	NCOIC	S	S	S	S	S	S	X	X	X	X	X	X	-	X	X	X	-	-	-	X	X	-	X	X
5	Joint Clerk	X	X	X	X	X	X	X	X	X	X	-	-	-	X	X	X	-	-	-	X	X	-	X	-
4	CMCC Clerk	S	S	S	S	S	S	X	X	X	X	-	-	-	X	X	X	-	-	-	X	X	-	X	-
3	TCSO	T	T	T	T	T	T	-	-	-	-	-	-	-	-	-	-	-	-	-	T	X	-	-	-
2	TS Clerk	T	T	T	T	-	T	-	-	-	-	-	-	-	-	-	-	-	-	-	T	X	-	-	-
1	SCP Cust	-	P	P	-	P	P	-	-	-	-	-	-	-	-	-	-	-	-	-	P	X	-	-	-
0		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

X = all documents - = no access for any classification
T = top secret documents only
S = secret and confidential documents only
P = only those documents subcustodied to that SCP

Figure D-1. Authorized Access Levels.

system (see Figure D-2). The purpose of this warning message is to remind the operator that COMMANDOC is to be used for official business only and that any unauthorized use of the system constitutes tampering with official records and is punishable under the Uniform Code of Military Justice. It further reminds the operator that certain elements of information are protected by the Privacy Act of 1974 and are not releasable to other parties nor may the personal information contained within the system be used by the operator for any purpose other than that for which it

ATTENTION!	ATTENTION!	ATTENTION!

Access to the information contained in this system is granted for official purposes only. Unauthorized access or access with the intent of disrupting the official records contained herein is a violation of the Uniform Code of Military Justice.

Certain items of information contained herein are protected by the Privacy Act of 1974 (5 U.S.C. 552a). Personal information protected by this act will not be released to unauthorized parties. Unauthorized disclosure is punishable by a fine of up to $5,000.

The act of entering your operator identification code (OPID) and password constitutes acknowledgement of reading this notice and your agreement to enter this system for official purposes only.

Do you understand and agree to these conditions? (Y/N)

Figure D-2. Warning Screen.

was intended. Finally, it reminds the operator that the use of a password constitutes agreement to the terms just as a signature would. Each operator must safeguard his password and change it on a regular basis. The COMMANDOC will notify the operator when his password is nearing expiration.

3. After entering a valid operator identification (OPID) and password, the COMMANDOC will display identification information of the operator who has logged on including when the last time and date was that the operator logged on and the date his password was last changed (see Figure D-3). If any of this information is not accurate the operator must notify the CMCC Officer immediately.

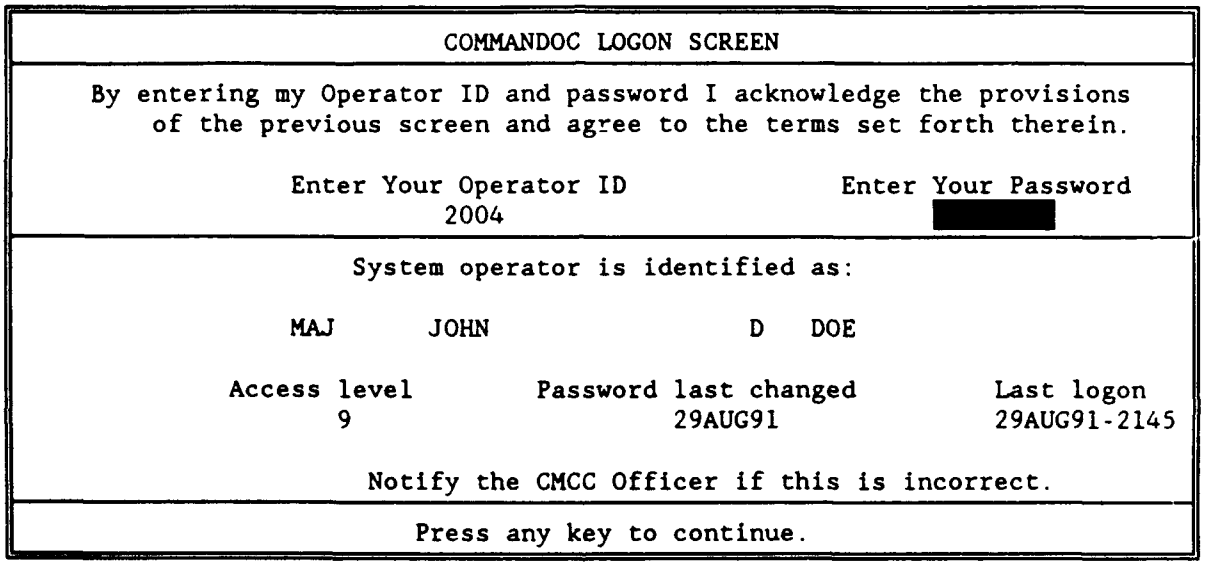


Figure D-3. Logon and Operator Identification Screen.

4. After passing the logon screen the operator will be presented with the first menu screen--the Main Menu (see Figure D-4). From the main menu the operator must select the type of action he needs to take. Actions are grouped by the various objects that they apply to: documents, secondary control points (SCPs), users, containers (safes and drawers), inventories, and utilities (such as assigning a new system operator, changing a password, or transferring or

receiving information from an SCP). The operator must select the number or letter of the necessary action. If the operator's access level does not match or exceed that required for the requested action, a warning message will be displayed and access will be denied.

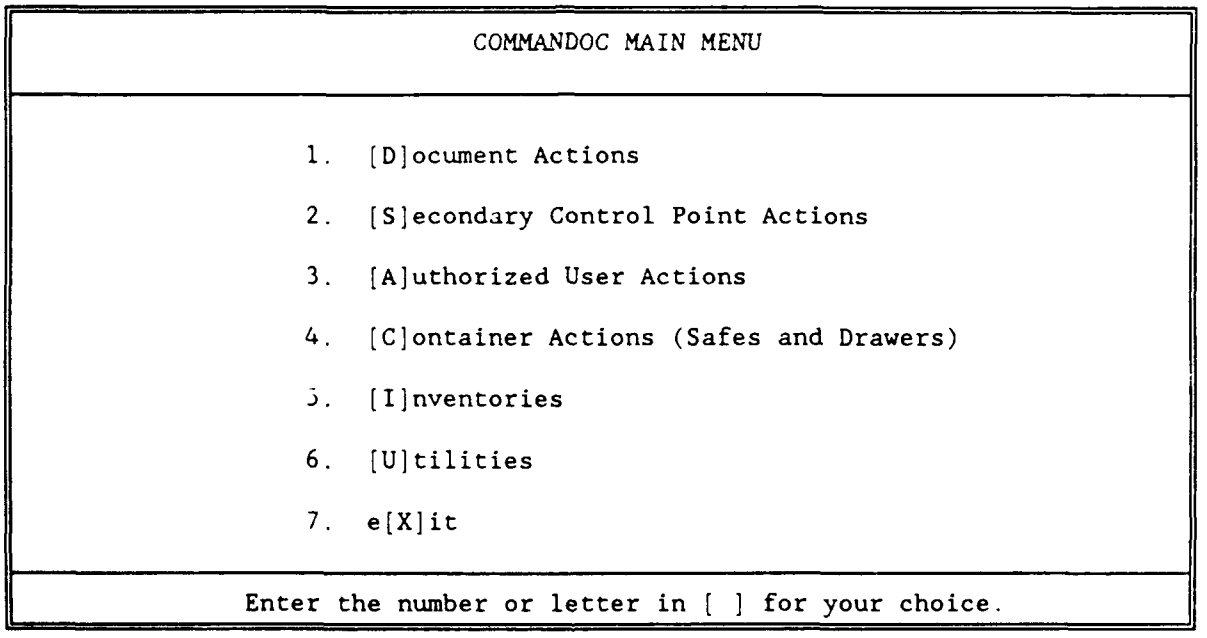


Figure D-4. COMMANDOC Main Menu.

5. Throughout the COMMANDOC system, all alphabetic characters are automatically converted to capital letters. This ensures that the data is entered in a uniform manner.

6. The operator may find it necessary to back out of a decision he has made or to escape from an endless loop. The operator can do this by entering zeros in the key field (i.e., "00-00000" for a control number or "0000" for a safe number).

SECTION 1. DOCUMENT ACTIONS

1.0 DOCUMENT ACTIONS MENU

Option 1 or D of the Main Menu will select the Documents Actions Menu. This menu will provide a wide variety of actions that the system operator can take that pertain to documents in the COMMANDOC system.

1.1 ADD DOCUMENTS

Option 1 or A is selected to add a new document to the system. A data entry screen appears (see Figure D-5) and the operator must fill in the blanks. The control number and copy number are automatically calculated and entered onto the screen.

DOCUMENT ENTRY SCREEN

Control#	Copy	Of	Class	NOFORN	SCI	NATO	CNWDI	Date Recd	#Pages	Reg Mail #
91-00100	1	1	C	N	N	N	N	30AUG91		

Originator	Orig Ser #	Doc Date	Declass
HQMC	LRP-9328-9	12JUL91	OADR

Subject
LOGISTIC REQR FOR OPLAN 123

Location	
Safe	Drawer
!	1

Short Title
LOG REQ OPLAN123

Print Cover Page now? (Y/N) Y

Figure D-5. Document Entry Screen.

If these numbers are incorrect for any reason (e.g., multiple copies of the same document), the correct information must be entered on top of the existing information. A message appears at the bottom of the screen to advise the operator of the information required for each field.

The default values for the special security conditions NOFORN, SCI, NATO, and CNWDI are defaulted to "N" for No. If a document has any of these extra security headings, type "Y" to change it to a Yes.

The "DATE RECEIVED" field will be automatically calculated to be the current date. This may also be typed over if it is not correct. Whatever date is entered (either the default date or a new one entered by the operator) is carried forward to the next document where it may be accepted or typed over again. This is helpful when the user is entering a number of documents that were received at one time--the date does not have to be reentered for each document.

A page count is required if the document classification is "T" for top secret. It is optional for secret and confidential. The default location for each new document entered is safe "! " and drawer "1". This flag will report the document as being maintained in the CMCC. The correct safe and drawer numbers should be entered if they are known. This information is utilized to prepare

inventories by safe and drawer for use in the emergency action plan.

The short title field is intended for entering numeric or abbreviated titles, such as NWPL numbers or directives numbers.

After completing all the fields, COMMANDOC will check that you are not entering data on a document that you should not have access to. For example, it will not allow you to enter a top secret document if you are not designated as the TSCO, alternate, or administrative assistant. If you are authorized to take the action indicated, the new document will be entered into the database and COMMANDOC will ask if you the information is correct. If the operator responds with a "Y", the system will ask if a cover page should be printed now. The normal response will be "Y" again. After the cover page has been printed, and after a negative response to either of the two preceding questions, the system will ask if there are more documents to enter at this time. An answer of "Y" will loop back through the process again and a negative answer will return to the Main Menu.

1.2 PRINT COVER PAGE

A cover page (OPNAV 5216/10) is normally prepared as the final step of entering a new document (see section 1.1). The occasion may arise where a new form must be created (the original form may have been lost, all spaces on the form may be completed, or the form may have jammed in the printer or

otherwise not properly completed). Option 2 or P will prepare a cover sheet for a document identified by the operator. This option calls a data entry screen that will ask for the document control number and copy number (top portion of Figure D-6). If a valid control number and copy number have been entered, COMMANDOC will display information about the document in order to verify that this is the correct document (see the bottom portion of Figure D-5). When the operator answers "Y" to the query "Correct information?

```
                    PRINT DOCUMENT COVER PAGE MENU

          Enter the Control Number and Copy Number of the
             document you need to print a cover page for.
                        CONT  NR        COPY #
                         91-00099           1


Control# Copy#   Of Class NOFORN SCI NATO CNWDI Doc Date
91-00099    1    1   S      F    F    F    F    15AUG90

Originator                                    Short Title
HQMC

Subject                                                Location
CLASSIFIED SUBJECT                                   Safe      Drawer
                                                      !            1

                    Correct information? (Y/N)
```

Figure D-6. Print Cover Page Data Entry Screen.

(Y/N)" the system will complete the cover page that has been properly aligned in the printer. If a incorrect control or copy number is entered, the system will advise the operator and permit another number to be entered. If the information

is incorrect and a "N" is entered, the system will return to the Document Menu.

1.3 MODIFY DOCUMENTS

Option 3 or M from the document menu will allow you to modify a document. This may be required for a variety or reasons, such as: moving the document to a different safe or drawer location; correcting the originator or title information; or downgrading the classification of the document.

Choosing this option will display a data entry screen that will ask the operator for the control number and copy number of the document to be modified. If invalid numbers are entered the system will notify the operator. If valid numbers have been entered, addition information about the document will be displayed and the operator may change the data as required (see Figure D-7). Certain fields may not be altered. The control number and copy number form the key field for each document and may not be change. If any of these fields are incorrect then the record of the document must be "destroyed" (entered on a destruction report) and the document reentered into the system with the correct information under a new control number.

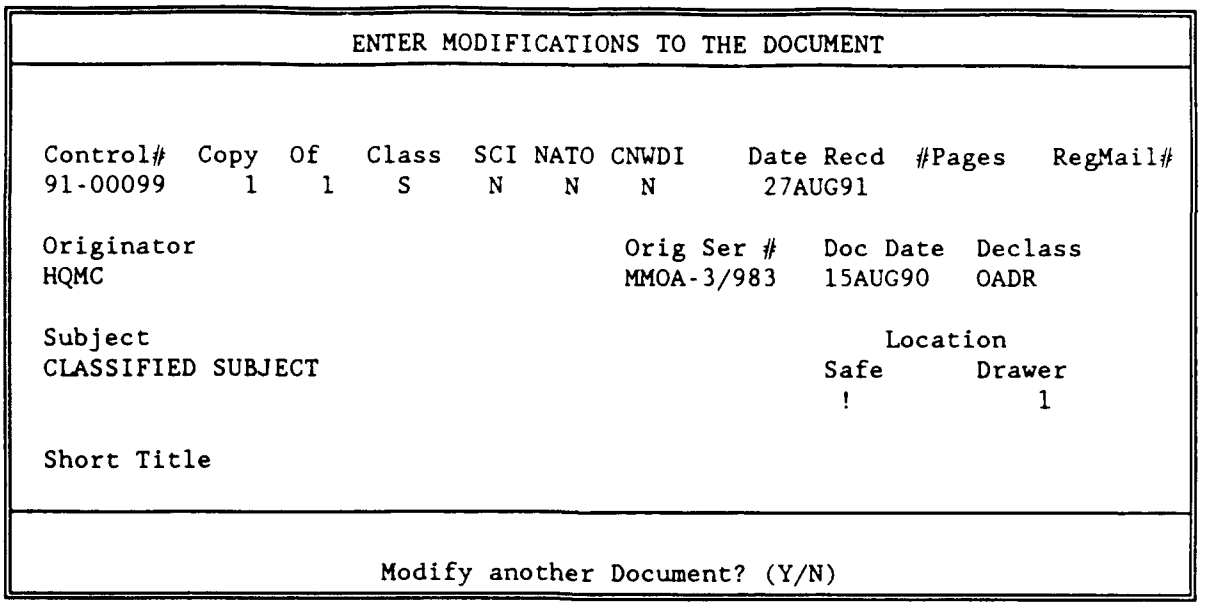


Figure D-7. Modify Document Data Entry Screen.

1.4 SUBCUSTODY MENU

Option 4 or S from the Document Menu will present the operator with another menu that will permit documents to be subcustodied to an SCP or to return documents from and SCP.

1.4.1 SUBCUSTODY DOCUMENTS

Option 1 or S from the Subcustody Menu will permit the operator to subcustody documents to an SCP. Before documents can be subcustodied, the designated SCP must already exist. See section 2.1 on adding a new SCP. The operator enters the control number and copy number of the document in the top portion of the data entry screen (see Figure D-8a). If the numbers entered are valid and a document is located, COMMANDOC will display further

information about the document in the center portion of the data entry screen (Figure D-8a). The lower portion of the

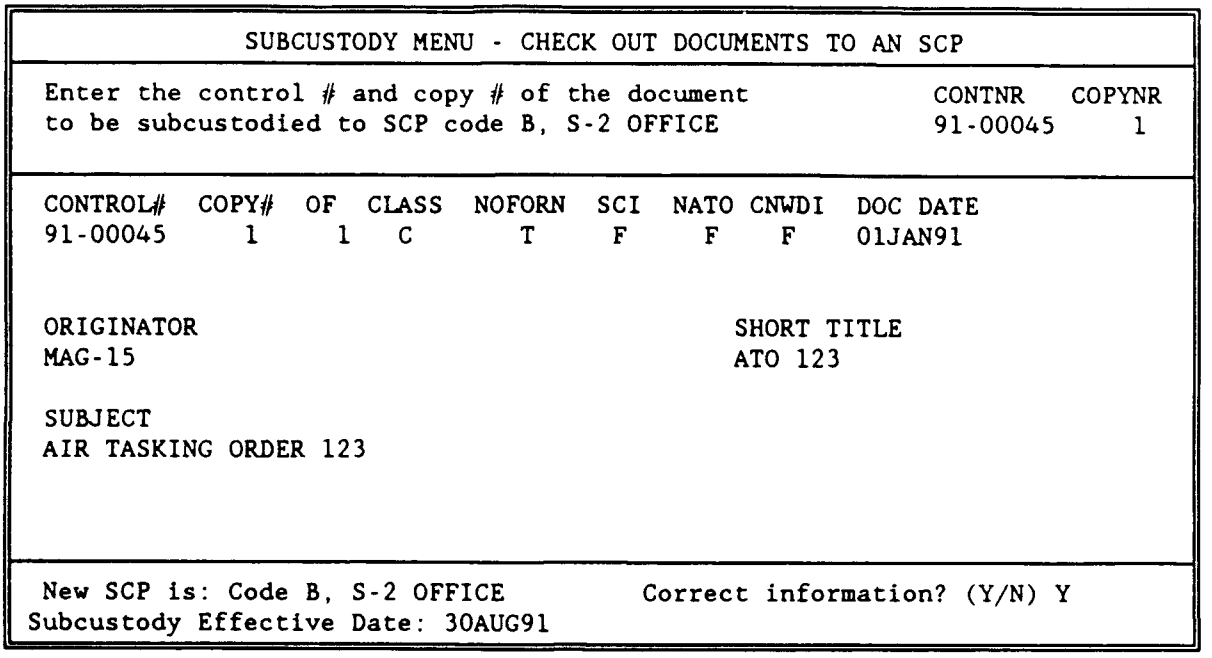


Figure D-8a. Subcustody Document Data Entry Screen.

screen will indicate the SCP that the document is being assigned to and the effective date of the subcustody. The default date of subcustody is the current date which can be accepted be pressing enter or can be overwritten if it is incorrect. This date will remain in memory until it is changed in order to eliminate reentering the date if multiple documents are being subcustodied to the same location during the same session. If the information displayed is correct, answer "Y" to the "Correct information?" prompt and the document will be reassigned to the designated SCP. If "Y" is entered, the lower portion of

the screen will change and ask if the operator wishes to subcustody more documents to the same SCP (see Figure D-8b). If the answer is "Y", the SCP Code will remain in memory as

New SCP is: Code B, S-2 OFFICE Subcustody Effective Date: 30AUG91	Correct information? (Y/N) Y More documents for same SCP? (Y/N)

Figure D-8b. Subcustody Document Data Entry Screen.

the destination for the next document. If the answer was "N", the lower portion of the screen will change again and ask in the operator wishes to subcustody documents to a different SCP (see Figure D-8c). If this is answered "Y",

New SCP is: Code B, S-2 OFFICE Subcustody Effective Date: 30AUG91	More documents for a different SCP? (Y/N)

Figure D-8c. Subcustody Document Data Entry Screen.

the cycle will repeat but will ask for a new SCP Code. If the answer is "N", the system will return to the Document Menu.

A physical signature for the subcustody action should be recorded on the official file copy of the cover page maintained in the CMCC. This serves two functions: first, it acts as a signed receipt of custody and second, it provides a chain of custody for the life of the document showing where the document has been routed and who has seen it.

1.4.2 RETURN DOCUMENTS

Option 2 of R from the Subcustody Menu returns subcustodied documents to the CMCC or reassigns them to another SCP. When this choice is selected, a data entry screen will request the control number and copy number of the document at the top portion of the screen. If invalid numbers are entered the system will notify the operator. If a valid document has been identified, COMMANDOC will display additional information about the document in the center part of the screen (see Figure D-9a)

```
SUBCUSTODY MENU-RETURN DOCUMENTS TO THE CMCC OR ASSIGN TO A DIFFERENT SCP

Enter the control # and copy # of the document to be      CONTNR    COPYNR
 returned to the CMCC or reassigned to another SCP:       91-00045      1


CONTROL#  COPY#  OF  CLASS  NOFORN  SCI  NATO CNWDI  DOC DATE
91-00045     1    1   C        T     F     F    F    01JAN91

ORIGINATOR                                    SHORT TITLE
MAG-15                                        ATO 123

SUBJECT
AIR TASKING ORDER 123

Subcustodied to SCP Code: B          Correct information (Y/N)?
          SCP Name: S-2 OFFICE
```

Figure D-9a. Return Subcustody Documents Data Entry Screen.

to ensure that it is the correct one. If the operator responds "Y" when asked if it is the correct document, the bottom portion of the screen will change (see Figure D-9b) and ask if the document is being returned to the CMCC or is

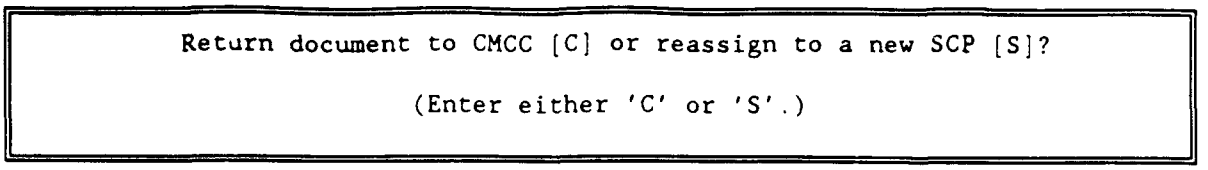


Figure D-9b. Return Subcustody Documents Data Entry Screen.

being reassigned to another SCP. A response of "C" will return custody to the CMCC and a response of "S" will prompt the operator to provide the new SCP Code.

1.4.3 EXIT

Option 3 or X from the Subcustody Menu exits and returns to the Document Menu.

1.5 CHECK DOCUMENTS IN OR OUT

Authorized users of documents held in the CMCC may check out documents and retain them in their personal safes (if so authorized). Unlike subcustoding a document to an SCP, accounting responsibility remains with the CMCC when a document is checked out. Option 5 or C from the Document Menu will provide another menu that will ask if the operator wishes to check out a document, return a document, or to exit the routine.

1.5.1 CHECK OUT A DOCUMENT

Option 1 or C from the Check Documents Menu will ask the operator for the user identification (i.e., SSN) of the individual who wishes to check out a document. The operator enters the user's SSN and COMMANDOC will display information

identifying that user (see Figure D-10a). If the information is verified as correct, the system will ask for the control number and copy number of the document (see Figure D-10b). If that document is found in the system, it

CHECK OUT DOCUMENT SCREEN								
SSN	Grade	LName	FName	MI	Office	Section		
123456789	MAJ	DOE	JOHN	D	MAG12	HQS1		
Clearance	Access	NOFORN	SCI	NATO	CNWDI			
S	S	F	F	F	F			
Correct information? (Y/N)								

Figure D-10a. Check Out Document Data Entry Screen.

CHECK OUT DOCUMENT SCREEN						
SSN	Grade	LName	FName	MI	Office	Section
123456789	MAJ	DOE	JOHN	D	MAG12	HQS1
Clearance	Access	NOFORN	SCI	NATO	CNWDI	
S	S	F	F	F	F	
Enter the doucment to be checked out.						
Control#	Copy#					
91-00101	1					

Figure D-10b. Check Out Document Data Entry Screen.

will be displayed in the center portion of the data entry screen for verification (see Figure D-10c). When the operator verifies the displayed information as the correct document to be checked out, the lower portion of the screen will ask for the new safe and drawer number where the document will be located (see Figure D-10d), and will clear and ask for the effective date of check out (see Figure D-10e). The current system date is the default but a different date may be entered if necessary. The COMMANDOC

```
                        CHECK OUT DOCUMENT SCREEN

   SSN      Grade   LName              FName              MI     Office Section
123456789   MAJ     DOE                JOHN                D     MAG12    HQS1

          Clearance      Access         NOFORN   SCI   NATO   CNWDI
              S             S              F      F     F      F

Control#  Copy#   Of Class NOFORN SCI NATO CNWDI Doc Date
91-00101    1     1   S      F    F    F    F    30AUG91

Originator                                    Short Title
CO 1STBN 2NDMAR                               APNX B OPLAN 234

Subject                                            Location
APPENDIX B TO OPLAN 234                         Safe      Drawer
                                                !            1

                        Correct document? (Y/N)
```

Figure D-10c. Check Out Document Data Entry Screen.

```
          Enter the new Safe Number S101 and Drawer Number 1
```

Figure D-10d. Check Out Document Data Entry Screen.

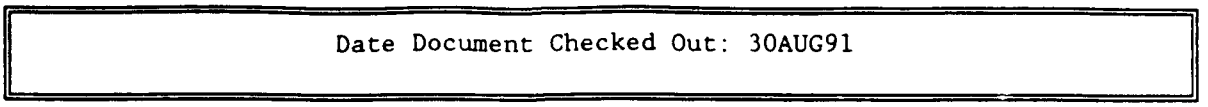


Figure D-10e. Check Out Document Data Entry Screen.

will check the authorized classification level of the user and the classification of the document and advise the operator if the user doesn't have a high enough clearance for the requested document. For example, a user with an authorization level of secret will not be allowed to check out a top secret document. If the user is authorized to receive the document, his SSN is recorded in the database as having custody of that particular document. This information will be displayed on any inventory prepared until he returns the document to the CMCC. This assists the CMCC Custodian in accounting for his documents during an inventory. The bottom portion will then clear and display a notice that the transaction has been accepted. After pressing any key to continue, a new menu will appear (Figure D-10f) asking if more documents are to be checked out to the same user or to a different user. The system will loop accordingly or exit, depending on the response provided.

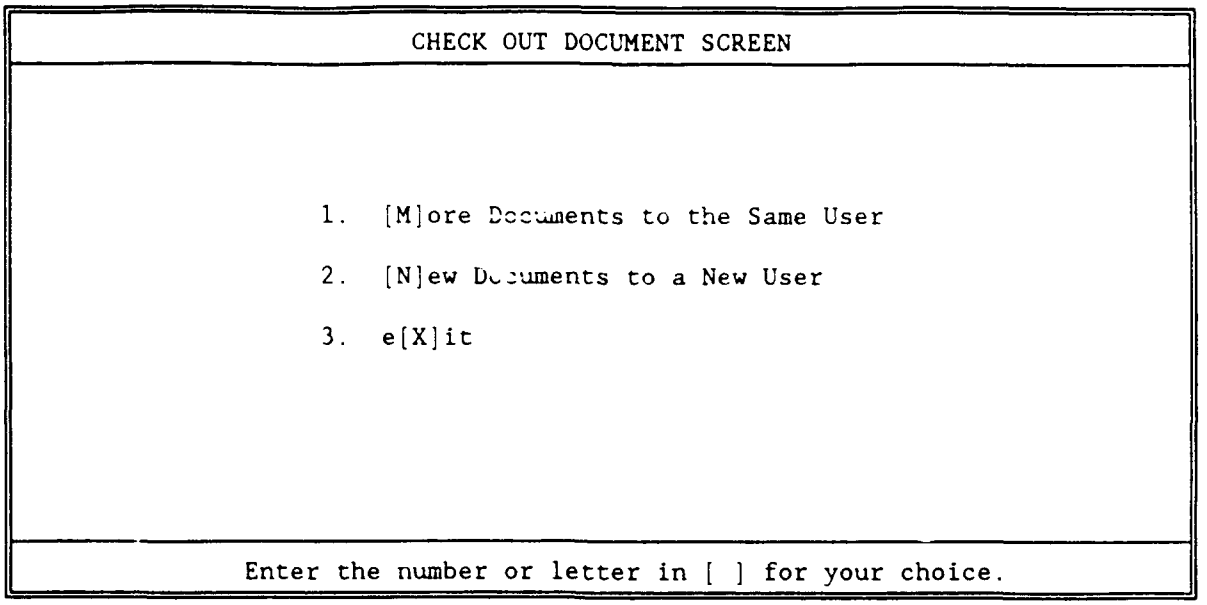


Figure D-10f. Check Out Document Data Entry Screen.

1.5.2 RETURN A DOCUMENT

Option 2 or R from the Check Documents Menu will return a document previously checked out back to the custody or the CMCC. This option will display a data entry screen (Figure D-11) that will ask for the control number and copy number of the document to be returned. Upon entry of valid numbers, the system will display the document information in the center part of the screen and ask for the new safe and drawer location of the document in the lower part of the screen. The operator must ensure that a valid safe and drawer number are entered.

```
                    CHECK IN DOCUMENT SCREEN

     Enter the control # and copy # of the document to be returned
                Control #: 91-00101     Copy #:     1

CONTROL#  COPY#  OF  CLASS  SCI  NATO CNWDI  DOC DATE
91-00101     1     1   S     F     F    F    30AUG91

ORIGINATOR                                   SHORT TITLE
CO 1STBN 2NDMAR

SUBJECT
APPENDIX B TO OPLAN 234

          Enter the new Safe Number: !002 and Drawer Number: 1
```

Figure D-11. Return Document Data Entry Screen.

1.5.3 EXIT

Option 3 or X from the Check Documents Menu will return to the Document Menu.

1.6 TRANSFER DOCUMENTS

Option 6 or T from the Document Menu will display a menu to choose the various actions associated with transferring documents (see Figure D-12).

1.6.1 CREATE A NEW REPORT

Option 1 or C from the Transfer Document Menu generates a new transfer report. A screen is presented displaying the last transfer report recorded and will compute the next sequential report. This computed number may be accepted or changed. The report number would be

changed, for example, to start a new sequence at the beginning of a new year. See Figure D-13.

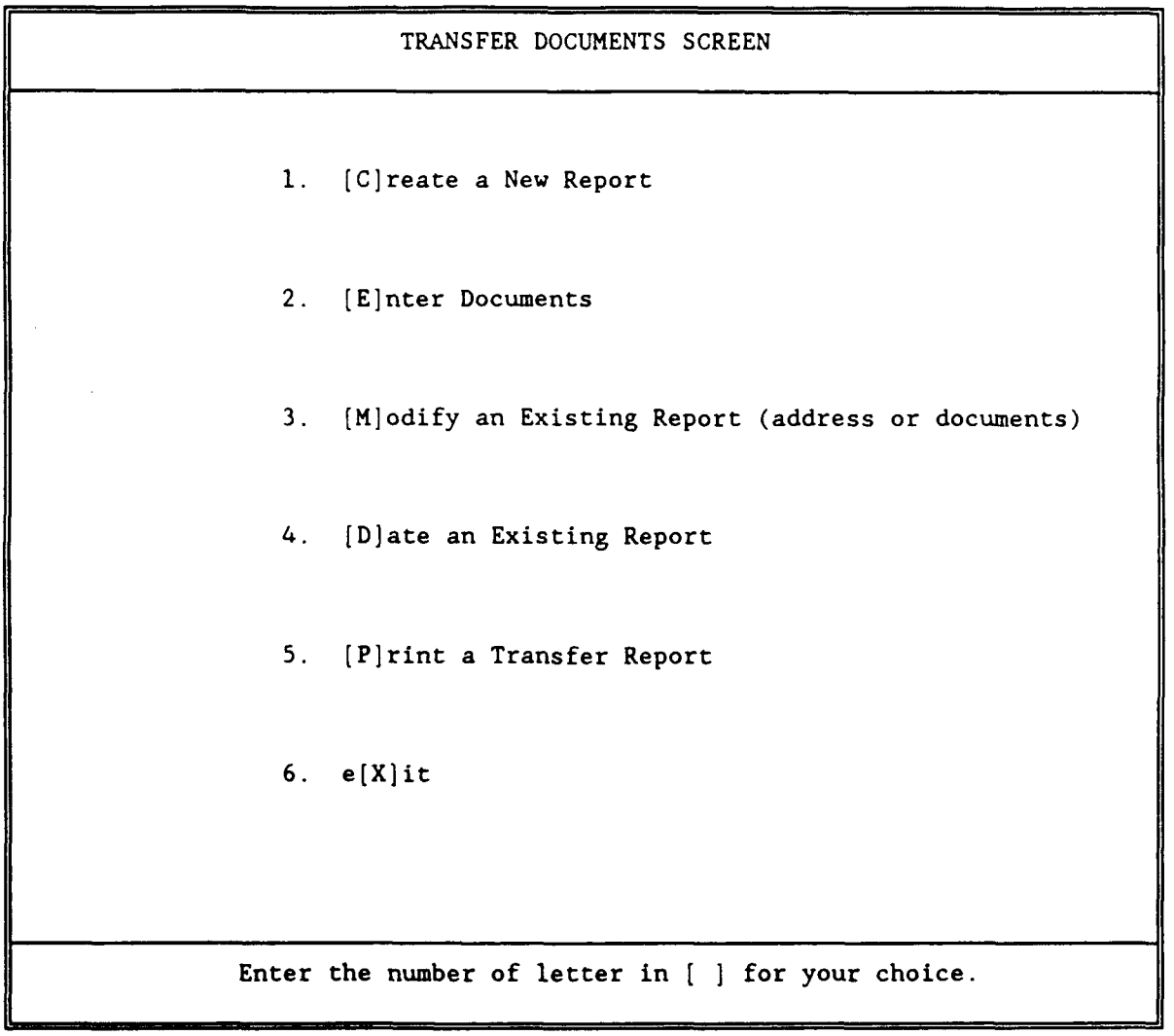


Figure D-12. Transfer Documents Date Entry Screen.

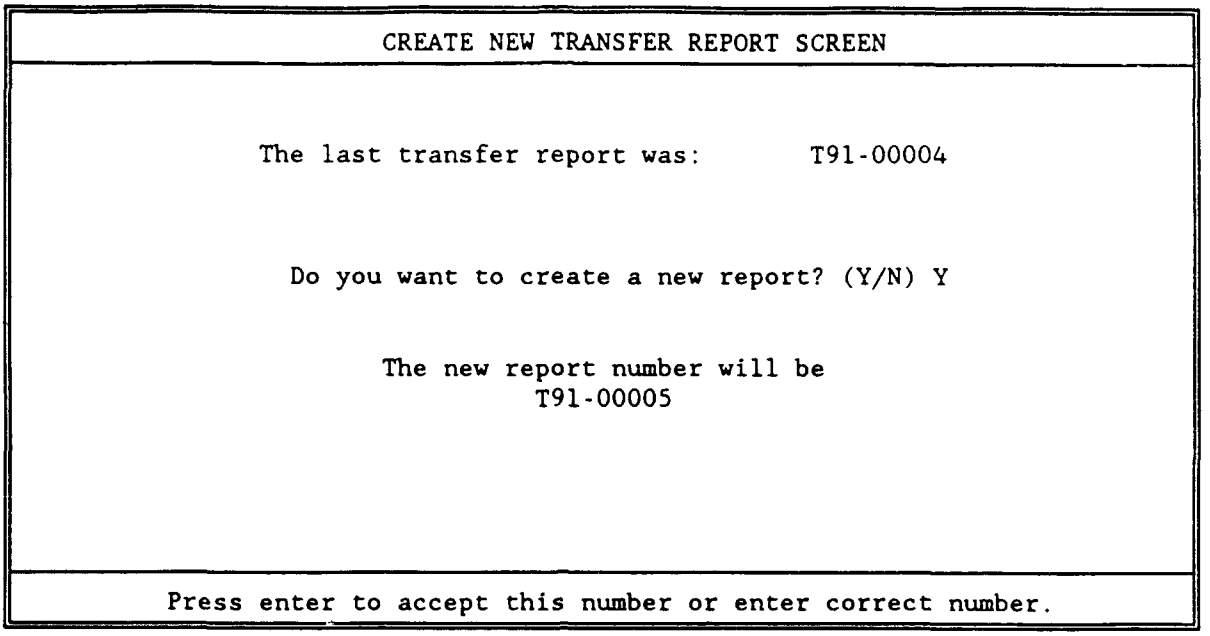


Figure D-13. Create New Transfer Report Data Entry Screen.

1.6.2 ADD DOCUMENTS

Option 2 or A from the Transfer Documents Menu will permit the operator to add documents to an existing transfer report. A data entry screen will ask for the transfer report number and then ask for the control number and copy number of the documents to be transferred (see Figure D-14). The document information will be display in the center of the screen to verify the document selected, and the bottom of the screen will ask the operator if the information is correct and if there are any more documents to enter to this report. An answer of "Y" will repeat the cycle, an answer of "N" will return to the Transfer Documents Menu.

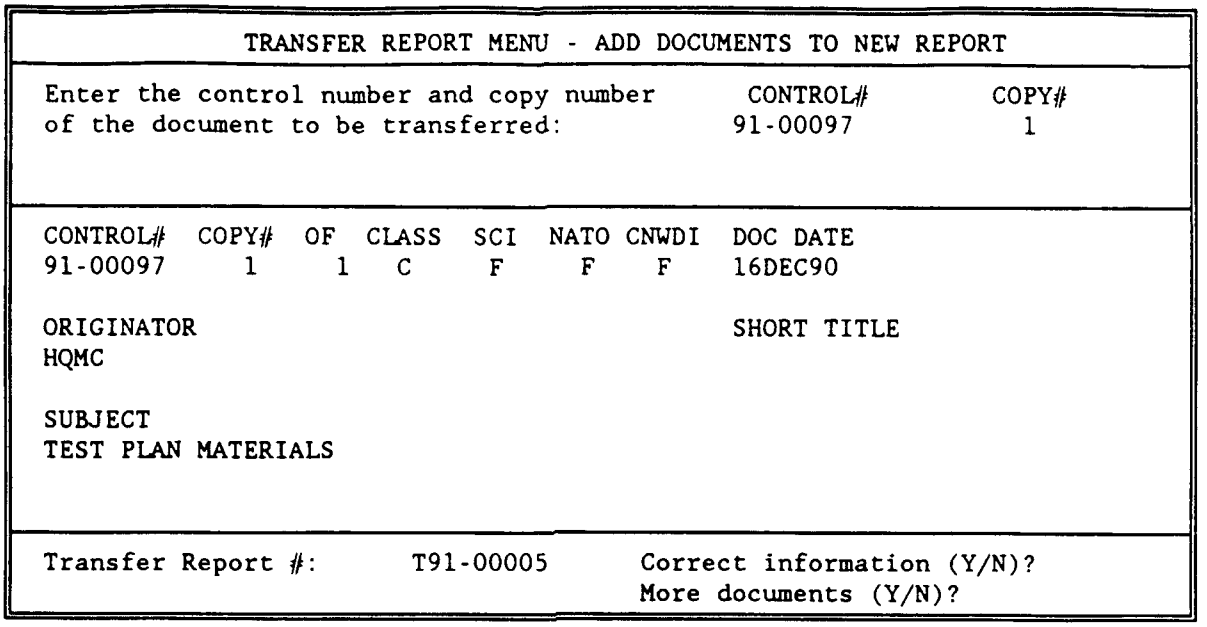


Figure D-14. Add Documents to Transfer Report Data Entry Screen.

1.6.3 MODIFY EXISTING REPORT

Option 3 or M from the Transfer Documents Menu will allow the operator to modify an existing report. A data entry screen will ask for the transfer report number of the report to be modified, and will then ask for the type of modification to be made: remove documents from the report or change the destination. See Figure D-15.

1.6.3.1 REMOVE DOCUMENTS

Option 1 or R from the Modify Report Menu provides a new screen that displays the document numbers of those documents identified for transfer on the indicated report. The format of this list is "control#/copy#" (see

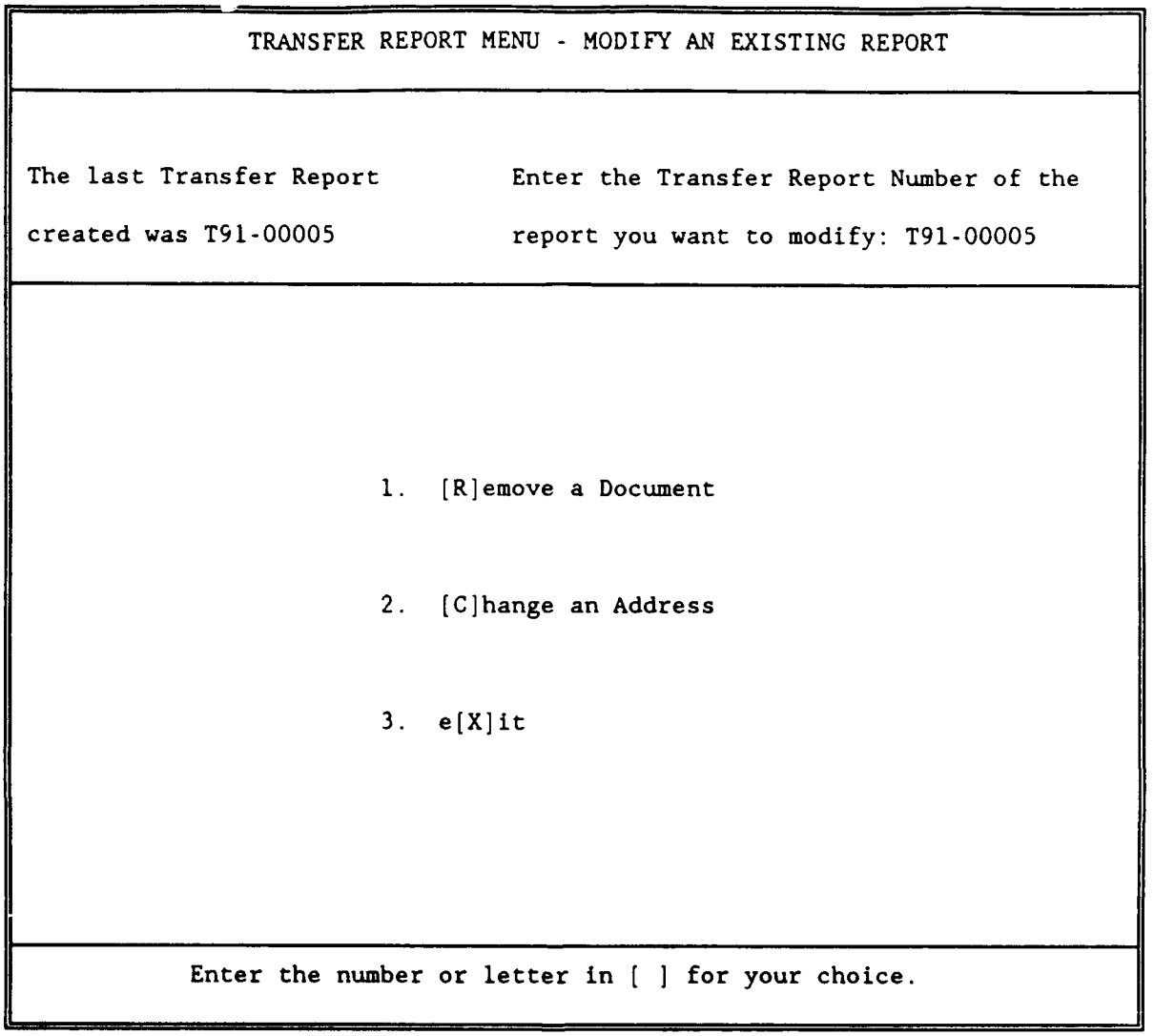


Figure D-15. Modify Transfer Report Data Entry Screen.

Figure D-16). The bottom portion of the screen will ask for the control number and copy number of the document to be removed from the report. When a valid document is entered the document's identifying information will be displayed in the center portion of the screen (see Figure D-17). The bottom portion of the screen will ask the user if the

information is correct and if there are more documents to remove from the report. A "N" answer to the first question and will discard the information previously entered; a "Y"

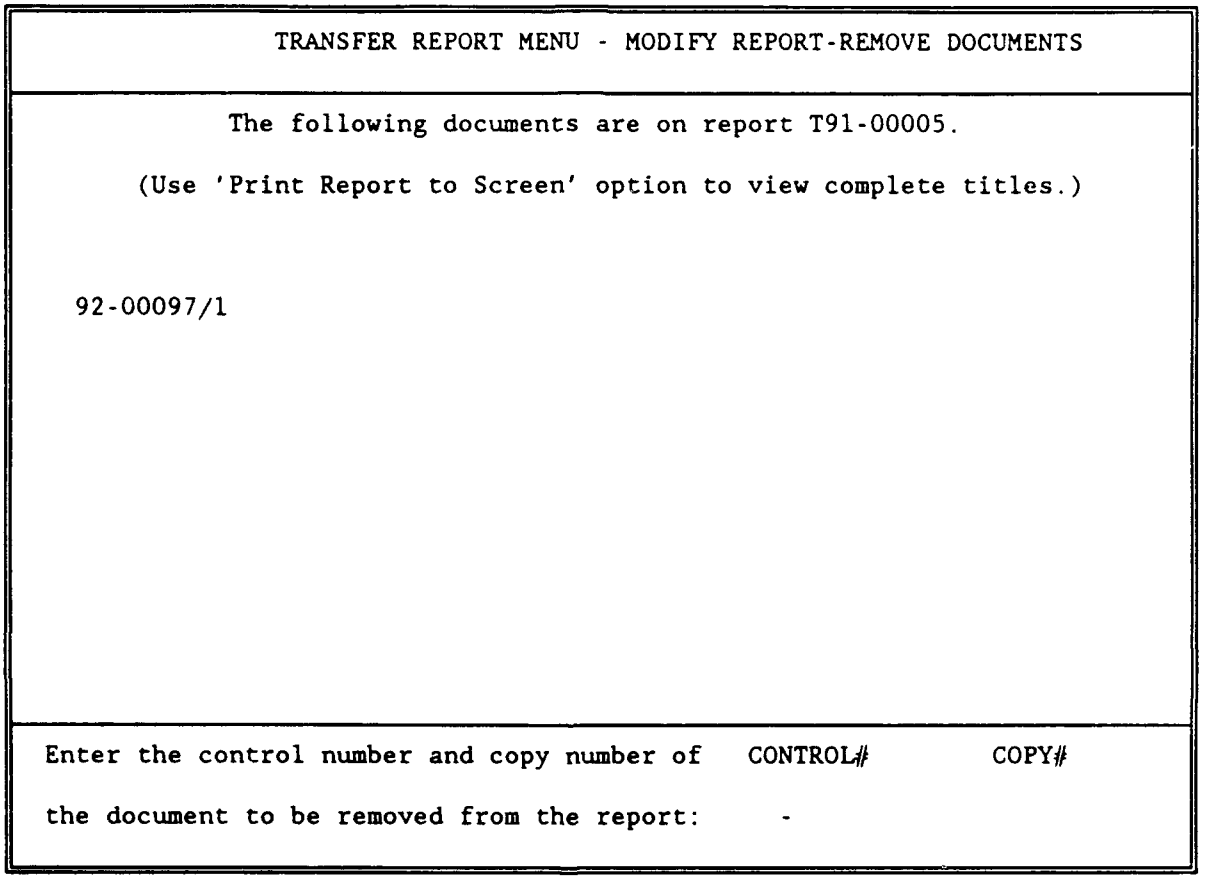


Figure D-16. Remove Documents from Transfer Report Data Screen.

answer will remove the document from the report. A "Y" answer to the second question will cause the system to repeat the process.

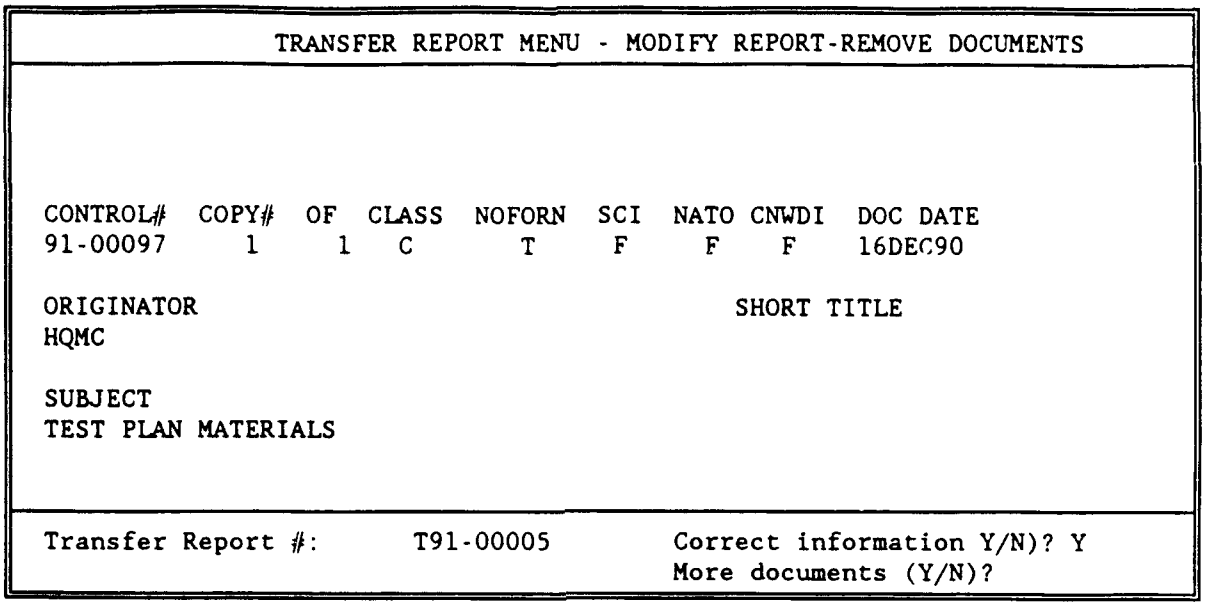


Figure D-17. Remove Documents from Transfer Report Data Screen.

1.6.3.2 CHANGE ADDRESS

Option 2 or C from the Modify Report Menu will permit the operator to change the destination of the transfer report. After asking for the report number to be modified, the system will display a screen that will show the old address and offer space for a new address to be entered. A completely new address must be entered, not merely the correction. See Figure D-18.

1.6.3.3 EXIT

Option 3 or X from the Modify Transfer Report Menu will exit and return to the Transfer Document Menu.

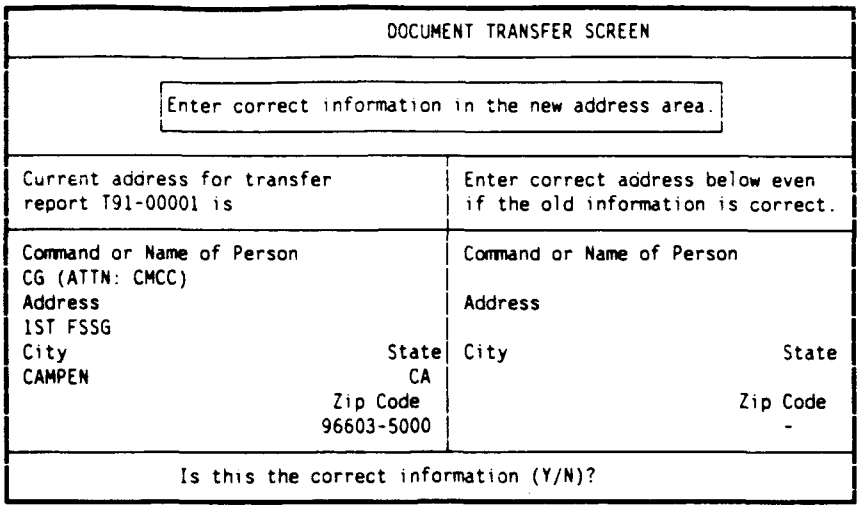


Figure D-18. Change Address of Transfer Report Data Screen.

1.6.4 DATE EXISTING TRANSFER REPORT

Option 4 or D from the Modify Transfer Report Menu permits the operator to date an prepared transfer report. Selecting this option will display a data entry screen that will list all pending transfer reports in the top portion of the screen (see Figure D-19). The COMMANDOC assumes a report is completed after a date has been added to it. The middle portion of the screen will ask for the report number of the report the operator needs to add a date to. The bottom portion of the screen asks for the date to be added to the selected report. This action will record the date of transfer to each of the documents listed on the specified report.

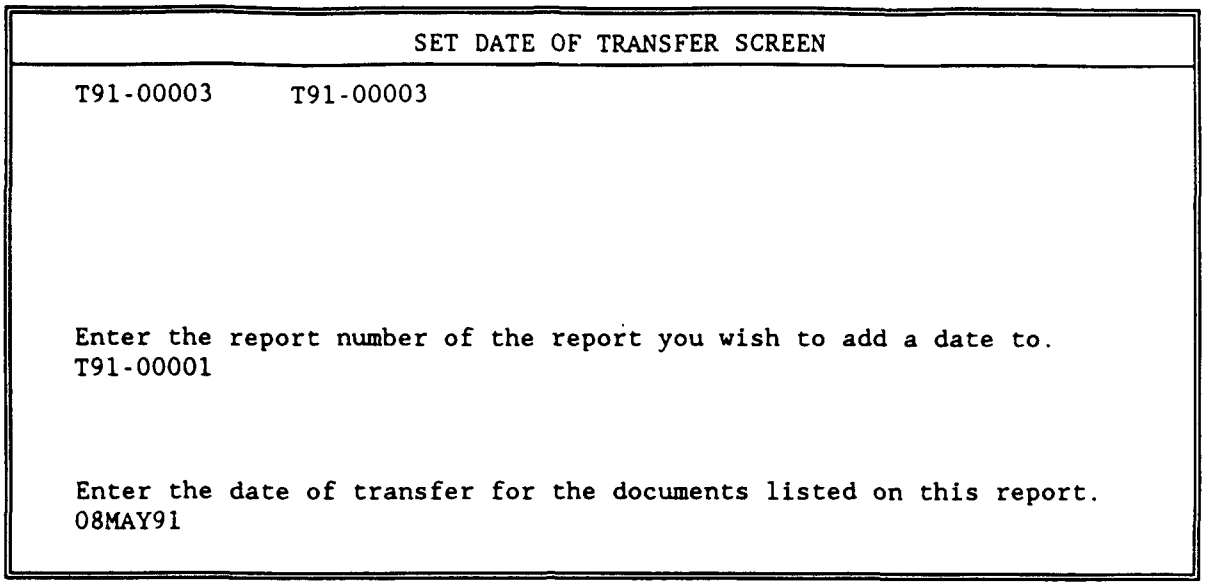


Figure D-19. Date Transfer Report Data Entry Screen.

1.6.5 PRINT TRANSFER REPORT

Option 5 or P of the Modify Transfer Report Menu will provide the screen shown in Figure D-20. It will provide the number of the last transfer report and ask for the report number of the report to be printed. After a report number is entered, a menu will appear in the center of the screen and ask if the user wants the report sent to the screen or to the printer. The format of the transfer report is designed so that the receiving command can fold the signed receipt copy with the originating command's address in position to show through the mailing window of a standard window envelope. This saves the receiving command from having to prepare an address on an envelope and ensures the receipt copy is returned to the proper command.

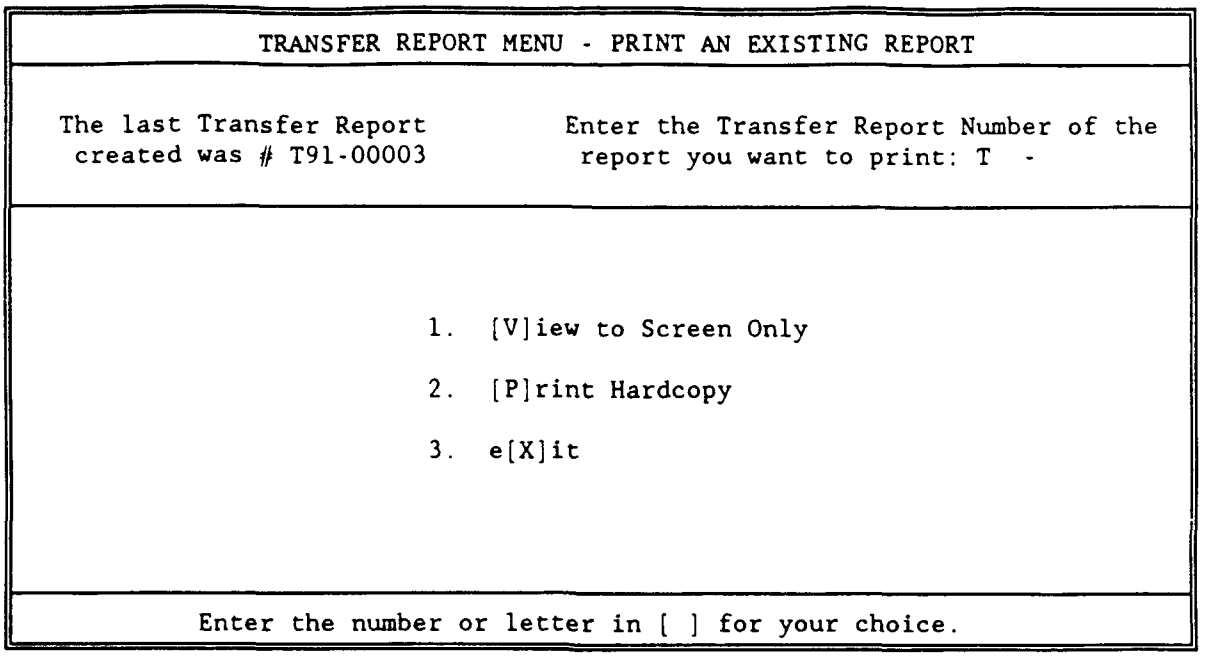


Figure D-20. Print Transfer Report Data Entry Screen.

1.6.6 EXIT

Option 6 or X from the Modify Transfer Report Menu will exit and return to the Transfer Document Menu.

1.7 DESTROY DOCUMENTS

Choice 7 or D from the Document Menu will display a menu that lists the various actions that can be taken when destroying documents.

1.7.1 CREATE NEW REPORT

Option 1 or C from the Destroy Document Menu generates a new destruction report. A screen is presented displaying the last destruction report recorded and will compute the next sequential report. This computed number may be accepted or changed. The report number would be

changed, for example, to start a new sequence at the beginning of a new year. See Figure D-21 below.

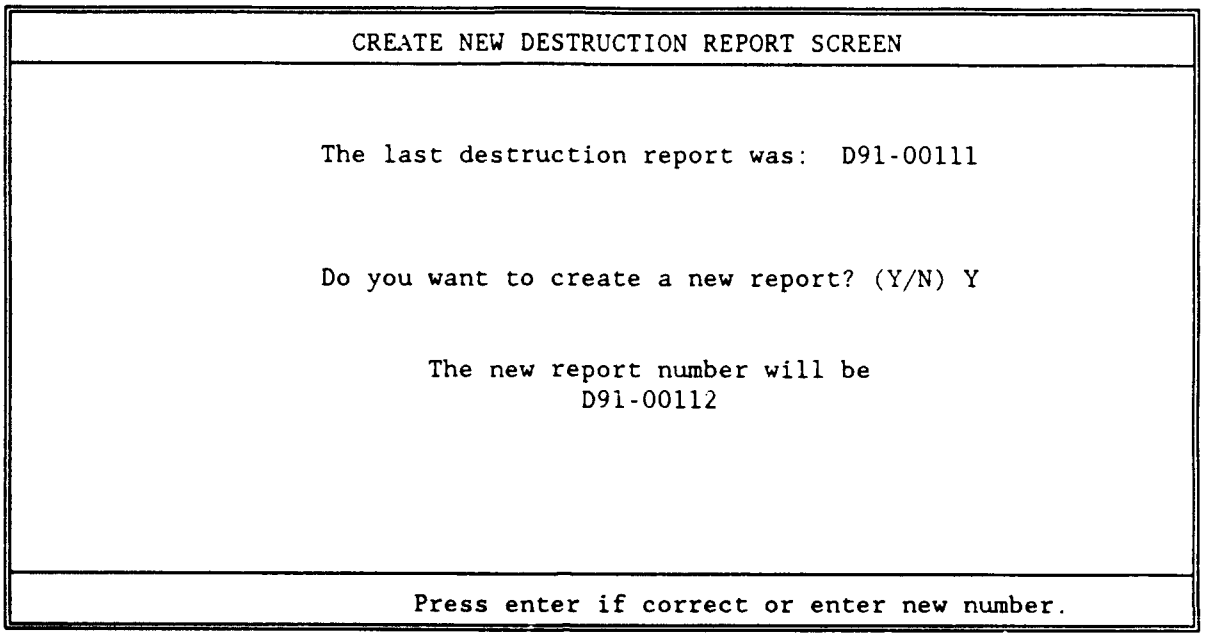


Figure D-21. Create New Destruction Report Data Entry Screen.

1.7.2 ENTER DOCUMENTS

Option 2 or A from the Destroy Documents Menu will permit the operator to add documents to an existing transfer report. A data entry screen will ask for the destruction report number and then ask for the control number and copy number of the documents to be transferred (see Figure D-22). The document information will be display in the center of the screen to verify the document selected, and the bottom of the screen will ask the operator if the information is correct and if there are any more documents to enter to this

report. An answer of "Y" will repeat the cycle, an answer of "N" will return to the Destroy Documents Menu.

```
          DESTRUCTION REPORT MENU - ADD DOCUMENTS TO NEW REPORT

 Enter the control number and copy number      CONTROL#        COPY#
  of the document to be destroyed:             91-00090          1

 CONTROL#  COPY#  OF  CLASS  NOFORN  SCI  NATO CNWDI  DOC DATE
 91-00090     1    2    S       T     F     F    F    12FEB90

 ORIGINATOR                                      SHORT TITLE
 NIC

 SUBJECT
 UNCONFIRMED SIGHTINGS 90/1


 Destruction Report #:   D91-00112    w Correct information (Y/N)? Y
                                      w More documents (Y/N)?
```

Figure D-22. Add Documents to Destruction Report Data Screen.

1.7.3 DATE EXISTING DESTRUCTION REPORT

Option 3 or D from the Modify Destruction Report Menu permits the operator to date a prepared destruction report. Selecting this option will display a data entry screen that will list all pending destruction reports in the top portion of the screen (see Figure D-23). The COMMANDOC assumes a report is completed after a date has been added to it. The middle portion of the screen will ask for the report number of the report the operator needs to add a date to. The bottom portion of the screen asks for the date to be added to the selected report. This action will record

the date of destruction to each of the documents listed on the specified report.

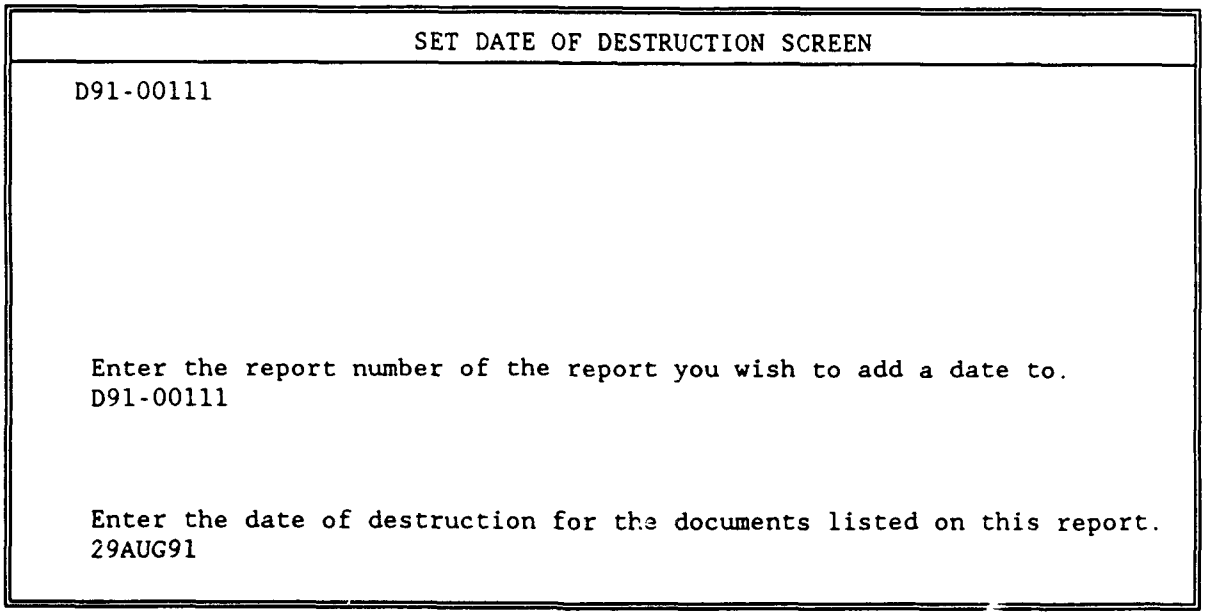


Figure D-23. Date Destruction Report Data Entry Screen.

1.7.4 PRINT TRANSFER REPORT

Option 4 or P of the Modify Destruction Report Menu will provide the screen shown in Figure D-24. It will provide the number of the last transfer report and ask for the report number of the report to be printed. After a report number is entered, the system displays the name of the organization conducting the destruction. This item is filled in with a default value based on information established during the installation of the system but may be overwritten if necessary. The system also asks for the operator identification (OPID) of the official authorizing the destruction (usually the CMCC Officer). When an

appropriate code is entered, the system will display the identity of the individual and this information will be printed on the destruction report. The system will ask for the OPID of the two witnesses performing the destruction. If they are authorized users within the system, their OPID will automatically recall their grade and name. If they are not entered as users their grade and name may be entered manually. This information will be printed on the destruction report.

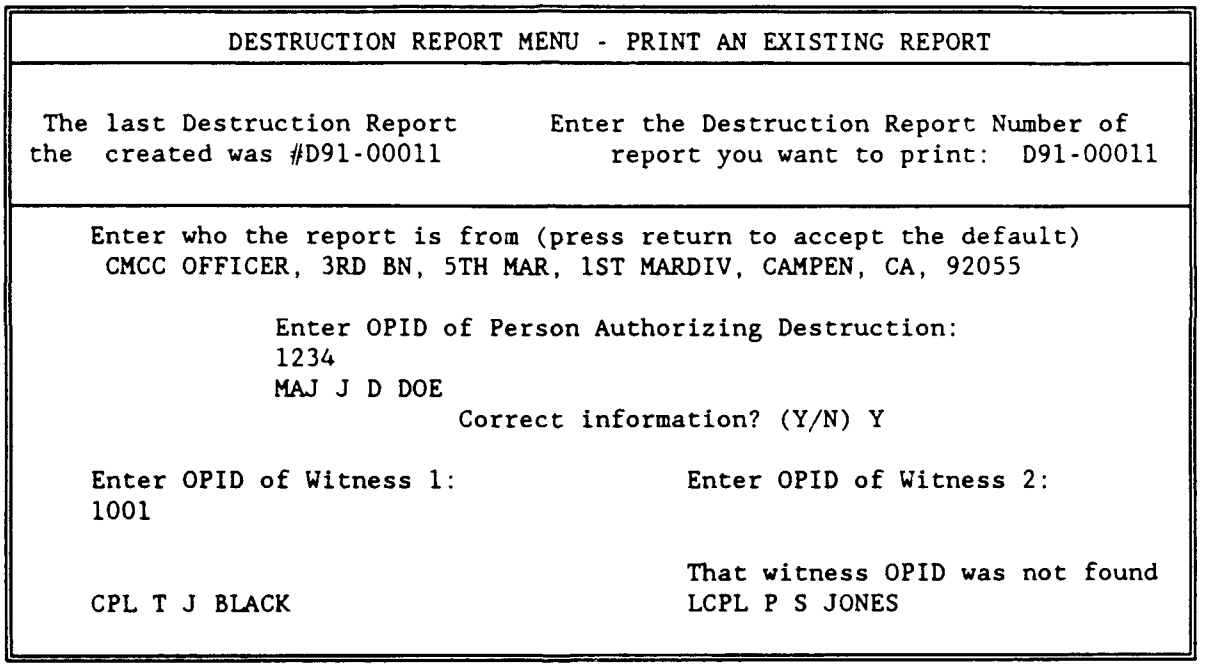


Figure D-24. Print Destruction Report Data Entry Screen.

1.7.5 EXIT

Option 5 or X from the Destroy Documents Menu exits and returns to the Document Actions Menu.

1.8 FIND DOCUMENTS

Choice 8 or S from the Document Menu will select the search option. This option allows the operator to search for one or more documents based upon a word contained in the title or by registered mail number. For example, a search could be made for all documents with the term "AMPHIBIOUS ASSAULT" or all documents with registered mail number "R198738266". This option supports the use of standard DOS wildcard characters (i.e., "%" will find any character at that position and "*" will find any character at that position or thereafter: "%RPT*" will find all references to a title beginning with any character followed by "RPT" and then followed by any combination of characters). The report of the found documents can be sent to either the screen or printer.

1.9 EXIT

Option 9 or X from the Document Menu will exit and return the operator to the logon process screen.

SECTION 2. SECONDARY CONTROL POINT ACTIONS

2.0 SECONDARY CONTROL POINTS MENU

Option 2 or S from the Main Menu will take the operator to the SCP Actions menu. Here the operator may choose to add, modify, or delete an SCP.

2.1 ADD AN SCP

Option 1 or A from the SCP menu allows the operator to add a new SCP to the COMMANDOC system. This action may only be performed by the CMCC NCOIC (system access level 6) or higher. Selection of this option will display a data entry screen that will advise the operator of the last SCP code assigned and will provide a list of current SCP codes if requested (see Figure D-25a). A follow-on data entry screen will collect the necessary

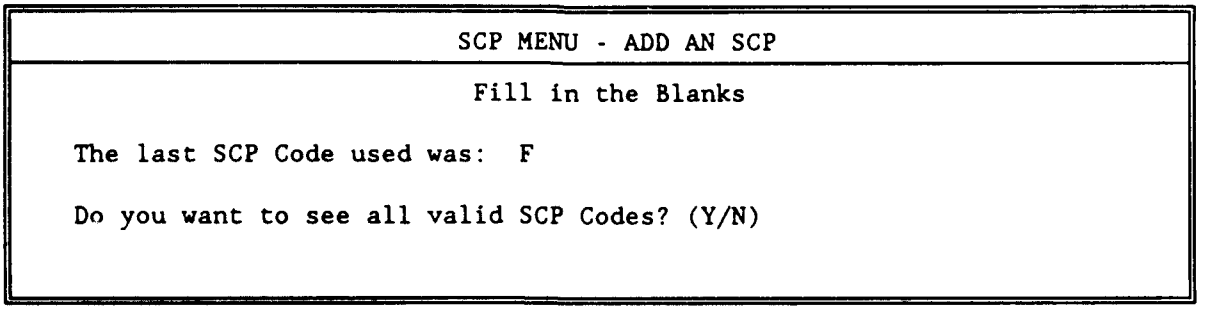


Figure D-25a. Add SCP Data Entry Screen.

data to establish a new SCP (see Figure D-25b). After verifying that the data is correct, the system will ask if there are more SCPs to be added and will repeat the process or return to the SCP Menu.

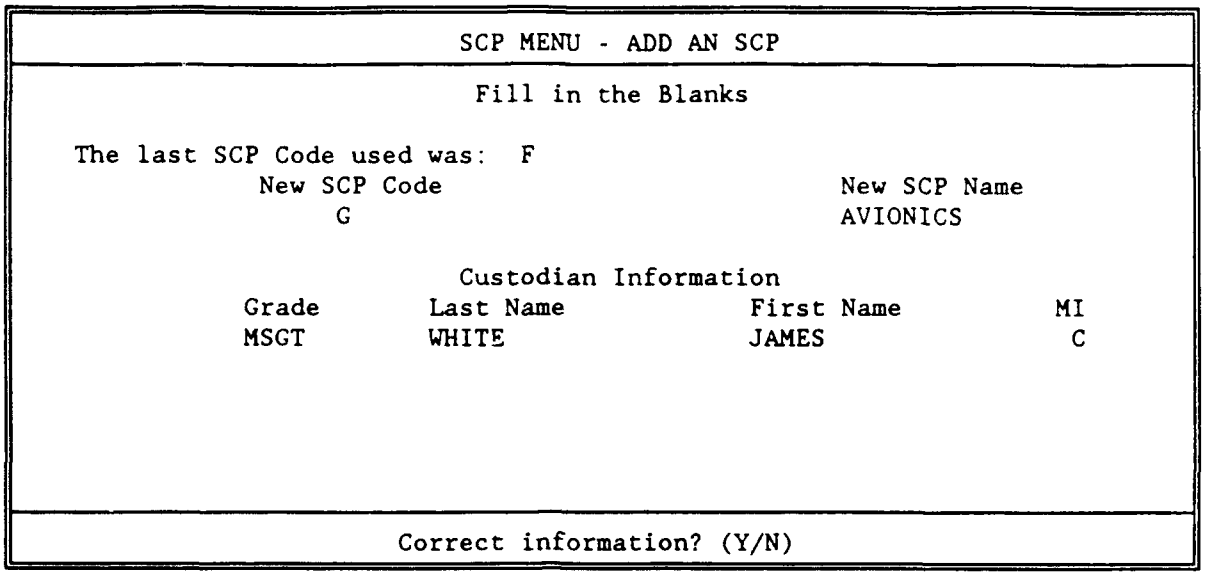


Figure D-25b. Add SCP Data Entry Screen.

2.2 MODIFY AN SCP

Option 2 or B from the SCP menu allows the operator to modify an existing SCP. The system will display the data entry screen shown in Figure D-26 and accept corrections to

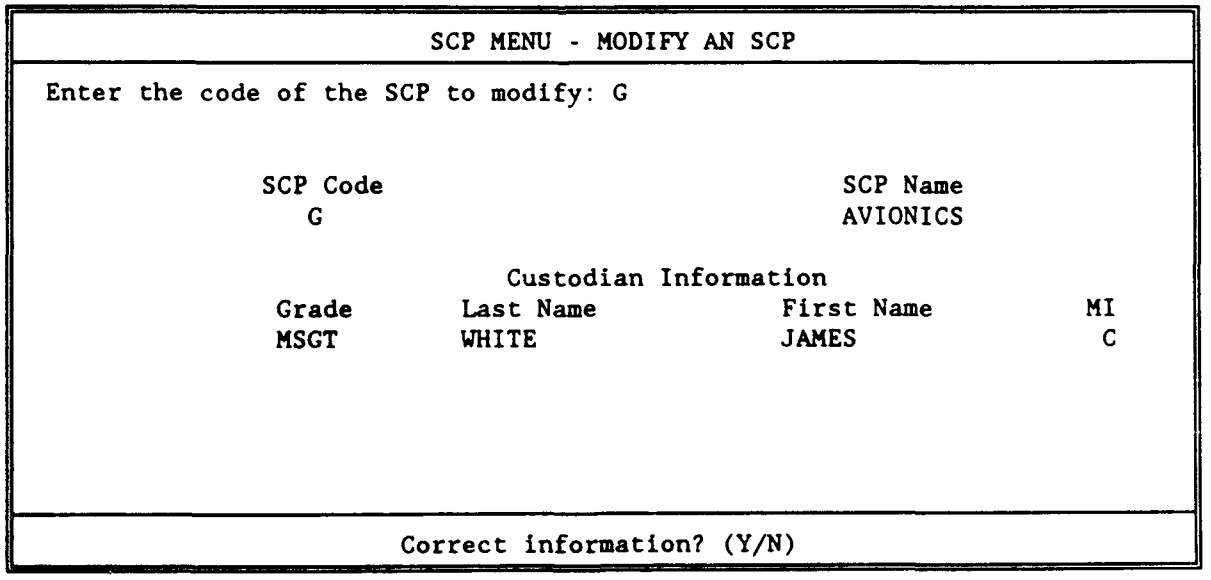


Figure D-26. Modify SCP Data Entry Screen.

existing information. Modification will be required when the custodian changes or if the name of the SCP changes. The SCP code is a key field and cannot be changed. If the code is incorrect, the SCP must be deleted and reentered as a new SCP. Access level 6 is required to modify an SCP.

2.3 DELETE AN SCP

Option 3 or D from the SCP menu allows the operator to delete an SCP from the COMMANDOC system. The system will display the top portion of the screen shown in Figure D-27 to receive the code of the SCP to be deleted. It will then display the SCP record to verify that the correct SCP has been selected. Deleting an SCP is a significant step, since all documents assigned to the SCP must be returned to the CMCC or reassigned to another SCP before the SCP can be

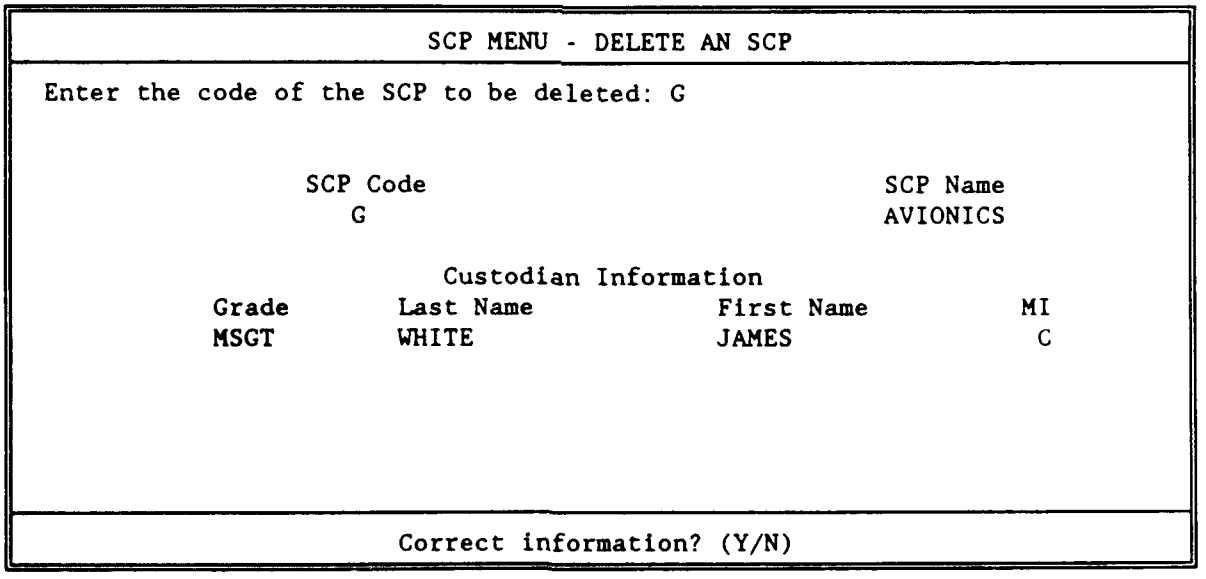


Figure D-27. Delete SCP Data Entry Screen.

deletec. Accordingly, system access level 8 or higher (CMCC Officer, alternate, or Security Manager) is required to complete this action.

2.4 EXIT

Option 4 or X from the SCP menu will exit the SCP menu and return one level to the main menu.

SECTION 3. AUTHORIZED USER ACTIONS

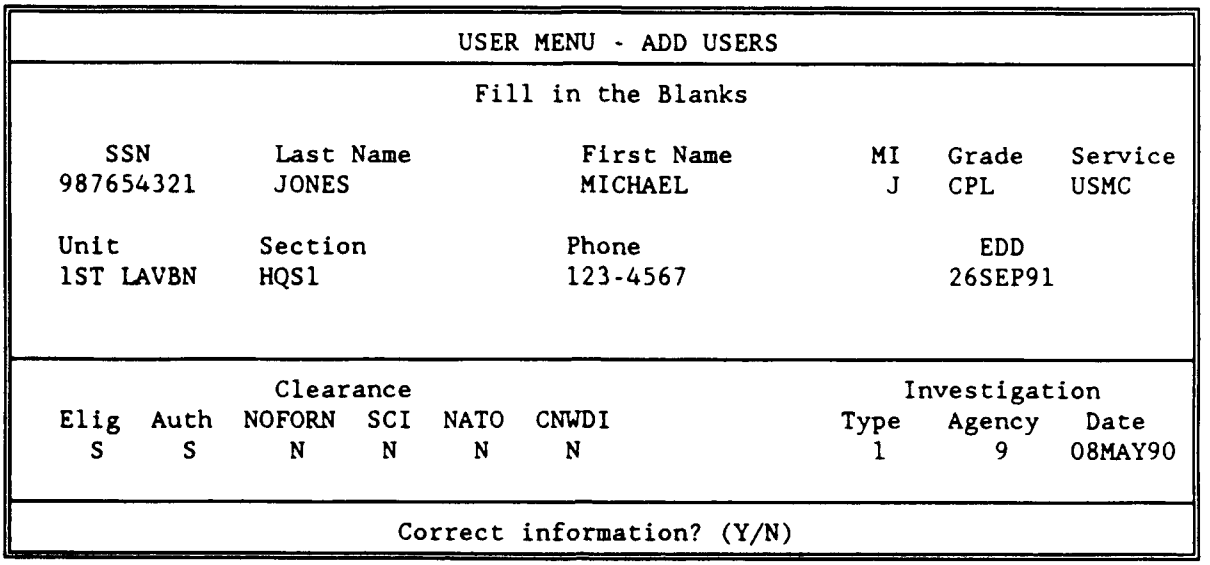
3.0 AUTHORIZED USERS MENU

Option 3 or U from the Main Menu provides the operator with a menu of options pertain to users. The operator may add, modify, or delete a user, or print a list of users (i.e., an access roster).

3.1 ADD A USER

Option 1 or A from the User Menu allows the operator to add a new user to the COMMANDOC system. This action may be completed by the CMCC Clerk (system access level 4 or higher). Upon selecting this option a data entry screen will appear and the operator must complete the information requested (see Figure D-28). Most of the fields are self-explanatory and some may be customized for each command. UNIT and SECTION codes may be abbreviated but abbreviations must be consistent as these fields will be used at a later time to sort and prepare reports (i.e., "S3" and "S-3" are two different codes). The information for the screen is obtained from verification from the appropriate office that the individual has a valid clearance and a need-to-know to be authorized access to classified material up to the level indicated on his clearance. Requests for clearance are forwarded to the DONCAF and may take several weeks to be responded to. The local commander may grant interim access pending a response from DONCAF. Exact procedures vary but

such interim access requests are normally approved by the Security Manager or his assistant.



USER MENU - ADD USERS

Fill in the Blanks

SSN	Last Name	First Name	MI	Grade	Service
987654321	JONES	MICHAEL	J	CPL	USMC

Unit	Section	Phone	EDD
1ST LAVBN	HQS1	123-4567	26SEP91

		Clearance				Investigation		
Elig	Auth	NOFORN	SCI	NATO	CNWDI	Type	Agency	Date
S	S	N	N	N	N	1	9	08MAY90

Correct information? (Y/N)

Figure D-28. Add User Data Entry Screen.

After the data screen is completed, the bottom portion will ask if the information is correct and if there are more users to enter at this time. The system will repeat the process according to the answers entered.

3.2 MODIFY A USER

Option 2 or M from the User Menu will provide a data entry screen to permit the operator to modify information on a user (see Figure D-29). The screen will ask for the user's SSN and then display that user's record. Local procedures must be established to initiate user modifications. Authorized changes might include: name change, promotion, change of unit or section, change of

phone, or a change to eligibility and authorized classification levels (i.e., clearance upgraded or downgraded). After the changes have been typed over the old information, the system will ask if the information is correct and if there are any more users to be modified at this time. The system will repeat the process according to the answers provided. The SSN is a key field and cannot be changed. If a user has an incorrect SSN he must be deleted from the system and reentered.

USER MENU - MODIFY A USER

Enter the SSN of the User to be modified: 987654321

SSN	Last Name	First Name	MI	Grade	Service
987654321	JONES	MICHAEL	J	CPL	USMC

Unit	Section	Phone	EDD
1ST LAVBN	HQS1	123-4567	26SEP91

	Clearance						Investigation	
Eligible	Authorized	NOFORN	SCI	NATO	CNWDI	Type	Agency	Date
S	S	T	F	F	F	1	9	08MAY90

Correct information? (Y/N)

Figure D-29. Modify User Data Entry Screen.

3.3 DELETE A USER

Option 3 or D from the User Menu is selected to delete a user from the COMMANDOC system. This action may be a routine part of an individual's procedure upon transfer from the command or may be the result of administrative or disciplinary action that has revoked his clearance. Local

regulations must direct the exact procedures to be followed. The data entry screen (Figure D-30) will request the SSN of the user to be deleted and display that record in order to verify that it is the correct user. The system will ask for the effective date to drop the user and will display the current date as the default. Press enter to accept

```
                    USER MENU - MODIFY A USER

Enter the SSN of the User to be modified: 987654321

   SSN         Last Name      First Name          MI    Grade      Service
987654321      JONES          MICHAEL              J    CPL        USMC

Unit           Section        Phone                      EDD
1ST LAVBN      HQS1           123-4567                   26SEP91

                    Clearance                                    Investigation
Eligible   Authorized  NOFORN  SCI  NATO  CNWDI     Type  Agency     Date
   S           S          T     F     F     F         1      9      08MAY90

Emter the effective date to drop this user: 31AUG91

                    Correct information? (Y/N)
```

Figure D-30. Delete User Data Entry Screen.

this date or type over it with a different one. The bottom portion of the screen will ask if the information is correct and if there are more users to be deleted at this time and will repeat the process depending upon the answers provided. If the information is correct, the user's record will be flagged as inactive but will remain on file in the COMMANDOC for two years. This means that this user's SSN cannot be used to check out documents and will not appear on the

roster of authorized users but an operator can still search the system for that SSN with the modify option should it be necessary to obtain clearance information regarding that individual (for example, in the case of an investigation).

3.4 LIST USERS

Option 4 or L from the User Menu permits the operator to generate a roster of current users and their authorized access levels. The menu that appears offers a variety of formats for this list (see Figure D-31). Choice 1 (or A) will provide one master alphabetical list. Choice 2 (or S) will provide one list divided by unit. Choice 3 (or I) will provide one separate list for each unit. This last option permits individual lists to be sent to unit leaders for verification and update.

```
                USER MENU - PRINT ACCESS ROSTER

                    1.  [A]lphabetical Listing
                    2.  Unit Roster  - [S]ingle Report
                    3.  Unit Rosters - [I]ndividual Reports
                    4.  e[X]it

              Enter the number or letter in [ ] for your choice.
```

Figure D-31. User List Menu.

3.5 EXIT

Option 5 or X from the User Menu will exit the User Menu and return one level to the Main Menu.

SECTION 4. CONTAINER ACTIONS

4.0 CONTAINER ACTION MENU

Option 4 or C from the Main Menu provides the operator with a menu of option the pertain to security containers--the safes and drawers that hold the classified documents.

4.1 SAFE ACTIONS

Option 1 or S from the Container Menu selects options for a safe. A safe must be created before action can be taken to any of the drawers within that safe. All safe actions may be completed by the CMCC Clerk (system access level 4 or higher).

4.1.1 ADD A SAFE

Option 1 or A from the Safe Menu allows the operator to add a new safe to the COMMANDOC system. A data entry screen will ask for information regarding the safe--the safe number and location. The bottom of the screen will ask if the information is correct and if there are any more safes to add at this time. The process will repeat as required depending on the answers provided. Local procedures should be established to ensure a uniform and systematic means of labeling all safes. A recommended system would be to use the first two digits of the safe number as the office or SCP location and the last two digits for the safe number within that office. For example: S301, S302, S303 would indicate safes 1, 2, and 3 located in the S3 office; A001, A002, A003

would indicate safes 1, 2, and 3 located in SCP A. The default safe number generated when a new document is entered is safe number "! ". This indicates that the document hasn't been assigned to a permanent location and remains within the CMCC. Any document with this indicator will appear at the beginning of an inventory.

4.1.2 MODIFY A SAFE

Option 2 or M from the Safe Menu is used to modify information about a safe. The safe number is a key field and cannot be changed, but the description/location may change. The bottom of the screen will ask if the information is correct and if there are any more safes to add at this time. The process will repeat as required depending on the answers provided. If the safe number is incorrect the safe must be deleted from the system and reentered as a new safe.

4.1.3 DELETE A SAFE

Option 3 or D from the Safe Menu is used to delete a safe from the COMMANDOC system. A data entry screen will ask for the safe number of the safe to be deleted. If a valid safe number is found, the safe's location description will be displayed and the bottom of the screen will ask if the information is correct and if there are any more safes to add at this time. The process will repeat as required depending on the answers provided. All documents must be

reassigned from the drawers of a safe before that safe can be deleted.

4.1.4 EXIT

Option 4 or X from the Safe Menu will exit and return the operator one level to the Container Menu.

4.2 DRAWER ACTIONS

The second option of the Container Menu selects options for a drawer. A safe must be created before action can be taken to any of the drawers within that safe. All drawer actions may be completed by the CMCC Clerk (system access level 4 or higher).

4.2.1 ADD A DRAWER

Option 1 or A from the Drawer Menu allows the operator to add a new drawer to an existing safe in the COMMANDOC system. A data entry screen will ask for information regarding the drawer. The bottom of the screen will ask if the information is correct and if there are any more safes to add at this time. The process will repeat as required depending on the answers provided. Local procedures should be established to ensure a uniform and systematic means of labeling all drawers.

4.2.2 MODIFY A DRAWER

Option 2 or M from the Drawer Menu is used to modify information about a drawer. A data entry screen will appear and ask for the safe and drawer number of the drawer to be modified. If a valid combination is entered the system will

display the current drawer information and ask the operator to make appropriate changes (see Figure D-32). The safe and drawers numbers are key fields and cannot be changed. If the drawer number is incorrect and needs modification, the drawer must be deleted from the system and reentered as a new drawer. The bottom of the screen will ask if the information is correct and if there are any more safes to add at this time. The process will repeat as required depending on the answers provided.

DRAWER MENU - MODIFY A DRAWER

Enter the safe and drawer number of the drawer you want to modify.

Safe Number	Drawer Number
S101	1

Enter the new responsible office for this drawer

Safe Number	Drawer Number	Responsible Office
S101	1	S1 OFFICER

Correct information? (Y/N) Y

Figure D-32. Modify Drawer Data Entry Screen.

4.2.3 DELETE A DRAWER

Option 3 or D from the Drawer Menu is used to delete a drawer from the COMMANDOC system. A data entry screen will ask for the safe and drawer numbers. If a valid combination is entered, the drawer information will be

displayed. The bottom of the screen will ask if the information is correct and if there are any more safes to add at this time. The process will repeat as required depending on the answers provided. All documents stored in a drawer must be reassigned before it can be deleted.

4.2.4 EXIT

Option 4 or X from the Drawer Menu will exit and return the operator one level to the Container Menu.

4.3 EXIT

Option 3 or X from the Container Menu will exit and return the operator to the Main Menu.

SECTION 5. INVENTORIES

5.0 INVENTORIES MENU

Choice 5 or I from the Main Menu will display the Inventories Menu on the screen (see Figure D-33).

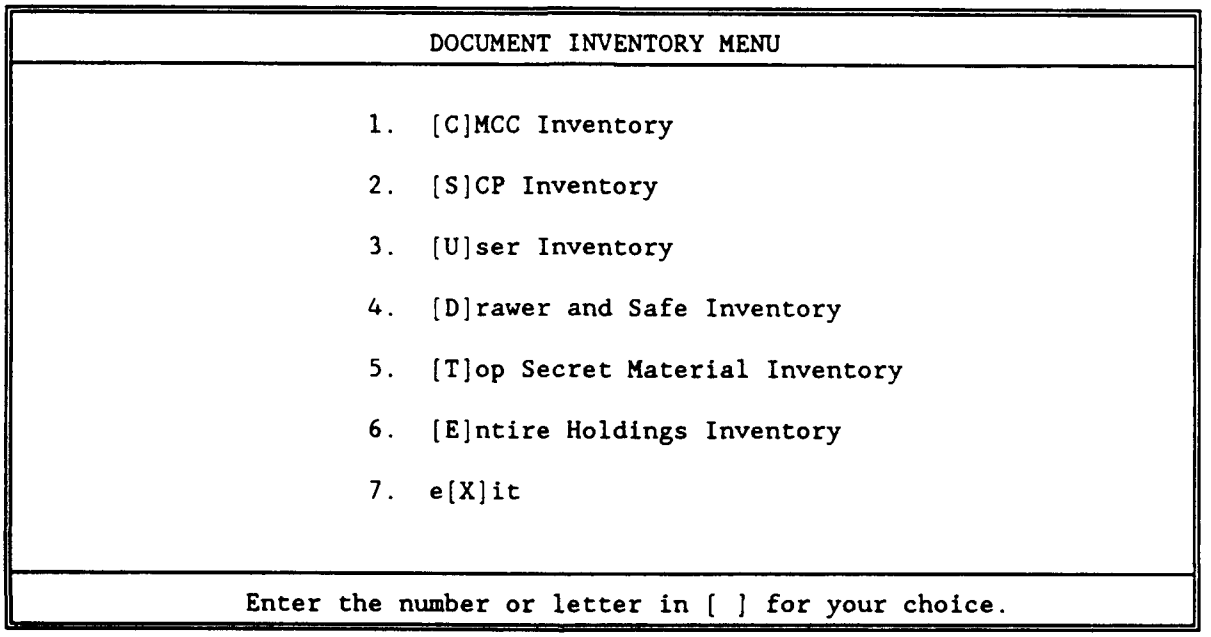


Figure D-33. Inventories Menu Screen.

5.1 CMCC INVENTORY

Choice 1 or C from the Inventories Menu will generate an inventory of all documents held in the CMCC. The operator may select either long title or short title format. If a document is checked out from the CMCC, the user's SSN is displayed to assist the CMCC Officer conduct the inventory.

5.2 SCP INVENTORY

Choice 2 or S from the Inventories Menu will generate an inventory of all documents assigned to a specific SCP. The

system will ask the operator for the SCP Code for which the inventory is requested. The operator may select either long title or short title format.

5.3 USER INVENTORY

Option 3 or U from the Inventories Menu will generate an inventory of all documents charged out to a specific user. The system will ask the operator for the SSN of the user for which the inventory is requested.

5.4 DRAWER/SAFE INVENTORY

Option 4 or D from the Inventories Menu will generate an inventory of all documents assigned to a specific drawer of a specific safe. This inventory is extremely useful for use with the Emergency Action Plan (EAP). This option provides a rapid system of identifying the documents that must be consolidated, moved, or destroyed.

5.5 TOP SECRET INVENTORY

Choice 5 or T from the Inventories Menu will generate an inventory of all top secret documents. This option will be useful to the Top Secret Control Officer (TSCO) when he must conduct an inventory or submit an inventory of top secret holdings to higher headquarters.

5.6 ENTIRE INVENTORY

Choice 6 or E from the Inventories Menu will generate an inventory of all active documents. The inventory will

indicate the location of each document (CMCC, SCP, or user). Short title or long title options are available.

5.7 EXIT

Option 7 or X from the Inventories Menu will exit and return the operator to the Main Menu.

SECTION 6. UTILITIES

6.0 UTILITIES MENU

Option 6 or U from the Main Menu provides the system operator with a menu of various utilities options (see Figure D-34).

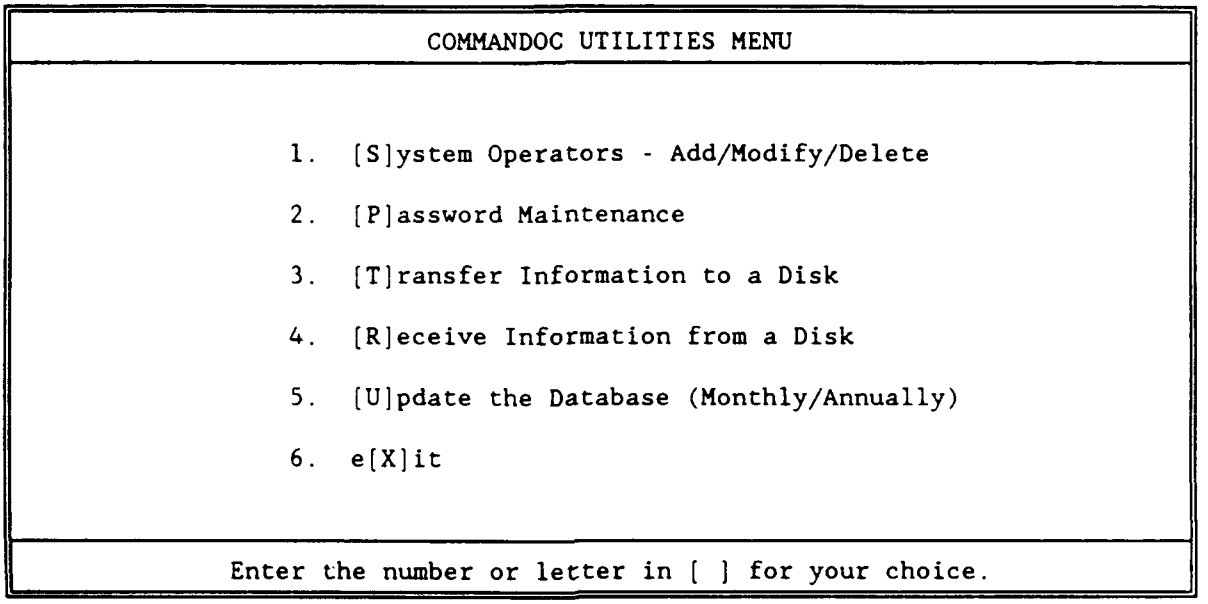


Figure D-34. Utilities Menu Screen.

6.1 SYSTEM OPERATOR

Option 1 or S from the Utilities Menu will permit the CMCC Officer of Security Manager (system access level 8 or higher) to assign a user status as a system operator. The term system operator is used to denote an individual who has been authorized to use the COMMANDOC system, as opposed to a user who is an individual authorized to utilize the services of the CMCC. Note that the new operator must first be an authorized user. The CMCC Officer should use the access

levels found in Figure D-1 to assign the new operator an appropriate code. Upon selection of this option, a data entry screen will request the user's SSN (see Figure D-35a). If a valid SSN is entered, the user's record will be displayed. This will assist the CMCC Officer in assigning a

OPERATOR MENU - ADD/MODIFY/DELETE OPERATOR ACCESS

[An operator must first be entered as an authorized user.]

Enter the SSN of the User to be authorized system access: 123456789

SSN	Last Name	First Name	MI	Grade	Service
123456789	DOE	JOHN	D	MAJ	USMC

Unit	Section	Phone	EDD
HQMC	MM	987-6543	

Clearance						Investigation		
Eligible	Authorized	NOFORN	SCI	NATO	CNWDI	Type	Agency	Date
T	T	T	F	F	F	4	9	17JUL79

Correct information? (Y/N)

Figure D-35a. System Operator Assignment Data Entry Screen.

level of access by displaying the clearance eligibility and authorized information. It also provides the opportunity to review the accuracy of the user's information. Return to section 3.2 if modifications are necessary. If the screen is verified as identifying the correct individual assignment, a message window will overlay the data screen (see Figure D-35b). This window will display the four digit Operator Identification code (OPID) that the COMMANDOC system generates. The new operator will automatically

receive a password. The password will be "PASSWORD" and the new operator must change it immediately. See section 6.2 for instructions on changing passwords. Both the OPID and password will be required every time the operator logs on to the COMMANDOC system. The CMCC Custodian will provide the access level for the new operator at the end of the prompt in the window. The CMCC Officer must enter his password to verify the assignment.

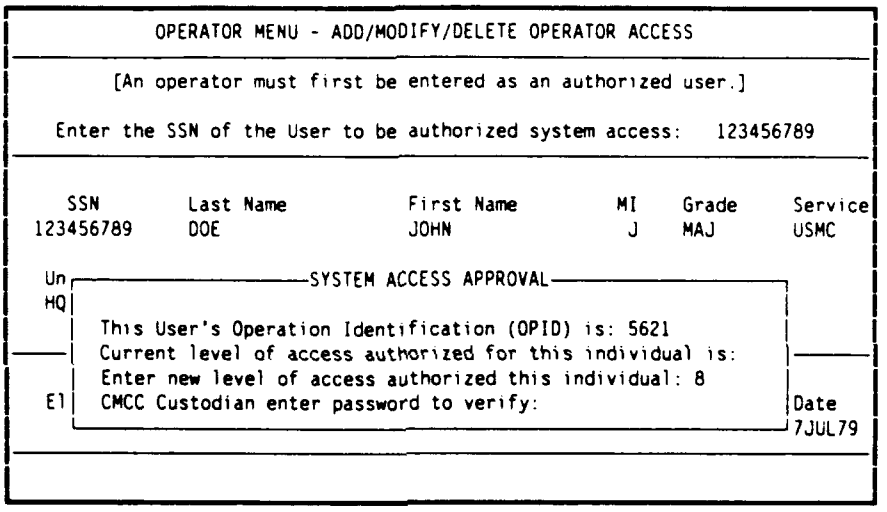


Figure D-35b. System Operator Assignment Data Entry Screen.

6.2 PASSWORD MAINTENANCE

Option 2 or P of the Utilities Menu will permit a system operator to change his password. Password management is an extremely important part of the COMMANDOC system and each operator must be familiar with the following procedures.

A password must be eight to ten characters long and should not be easily guessed. Some examples of bad passwords are:

AAAAAAAA - single letter or number repeated
12341234 - variation of the operator's OPID
123456789 - operator's SSN
28FEB1950 - birthdays, wedding anniversary, date of enlistment, RTD, EAS, etc.
COMMANDOC - name of the application being used
COMPUTER - easily guessed, common, computer-related word
PASSWORD - standard, preset password
WORDPASS - common variation of preset password

Some examples of good passwords are:

KAM2DOUR - mixed spelling and numbers; non-standard spelling
DUC$PS&3 - mixed letters, numbers, and special characters (but may be hard to remember)

Any proper word is a bad choice for a password because programs exist that can run a dictionary through the password algorithm and test for valid passwords. When a regular word that has been selected for a password is entered, it will encrypt in the same manner as an authorized user and permit access.

In order to prevent an operator from forgetting his password and becoming locked out of the COMMANDOC system, each operator should secure a copy of his password in an envelope (similar to a combination change envelope) and store it within a safe in the CMCC. Instructions on the envelope should prohibit anyone other than the authorized operator from opening the envelope, and any evidence of tampering with the envelope must be reported to the CMCC Officer immediately.

When a password is entered into the COMMANDOC it is immediately encrypted and the encrypted version compared with that operators encrypted password on file. If the passwords do not match, the operator will have two more attempts to correctly enter his password. After three attempts, the operator will be rejected from the system.

A password is dated when it is created and must be changed every six months. When a successful password is entered an information screen will notify the operator of the identity of the logged on operator. This identity screen will include the date the password was last changed. If the password is within ten days of expiring, a notice will be passed to the operator advising him to change his password. After 180 days, the system will automatically force the operator into the password maintenance option. If an operator logs on to the system with a password that is over 200 days old his access will be revoked and he will be locked out of the system.

Selection of this option will display a data entry screen (see Figure D-36). The upper portion of the screen will ask for the user's OPID and SSN. If a valid combination is entered, the system will display the individual's data record. This provides an opportunity for the individual to review his record and update information as required. See section 3.2 for modifying user's records. If the individual is verified as correct, the system will

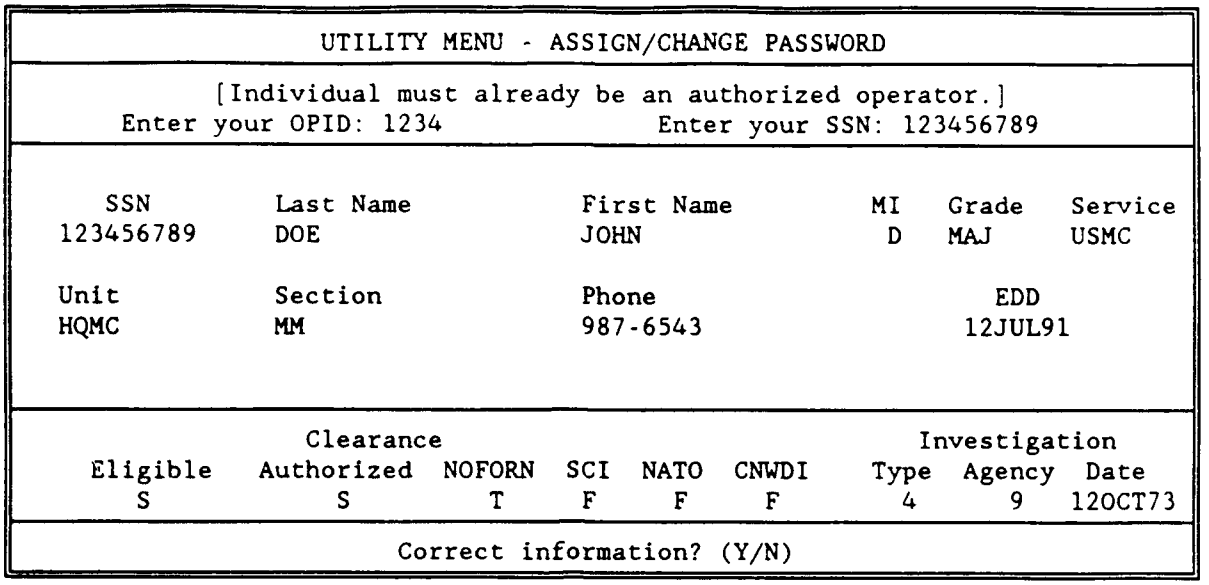


Figure D-36. Password Maintenance Data Entry Screen.

clear the screen and ask the operator to enter his password, and then to reenter it again. If the two entries match, the system will direct the operator to enter the new password, then to reenter it again. If the two entries match, the new password will take effect.

6.3 TRANSFER INFORMATION

Option 3 or T From the Utilities Menu allows the operator to transfer information to an SCP. This action may be initiated by the CMCC Clerk (system access 4 or higher). An example of this action would be downloading a database of all the documents held by an SCP in order to start an extension of the COMMANDOC within a command. This option could also be used to transfer records of documents recently subcustodied to the SCP.

Upon selecting this option the system operator must fill out the information on the data entry screen. The COMMANDOC will transfer the files to a floppy disk that can then be removed and transported to the remote system. One there, it will be uploaded following the instructions in section 6.4.

6.4 RECEIVE INFORMATION

Option 4 or R from the Utilities Menu is utilized to receive information from a remote source. Examples of this are an SCP receiving information from the CMCC to start an extension of the COMMANDOC within a command, or for an SCP to send information to the CMCC concerning the documents that the SCP has destroyed.

Upon requesting this option, the system operator must complete the information requested on the data entry screens.

This action must be executed by the CMCC NCOIC (system access 6 or higher) or by an SCP Custodian for only the documents in his SCP.

6.5 UPDATE THE DATABASE

Option 5 or U of the Update Database Menu opens a variety of options for the system operator. These actions are reserved for the CMCC Officer (system access 8 or higher).

6.5.1 WEEKLY UPDATE

This report provides the CMCC Officer with an usage report of system operators who have used the system since the last report was generated. This audit function is useful to ascertain if anyone has been attempting to use the system after hours, or to obtain historical data on the usage of the system. The usage report should be pulled weekly in order to prevent excessive disk space from being taken up by this growing file.

6.5.2 MONTHLY UPDATE

This option generates two reports. The first is a new access roster listing all current authorized users of the system and their authorized level of access. The second report is a similar list of authorized operators of the COMMANDOC system.

6.5.3 ANNUAL UPDATE

This option performs routine annual maintenance on the database and should be run on the first workday of each calendar year. It searches the database and purges it of the records of destroyed documents and transferred users more than two years old (five years for top secret documents). It is important to perform this annual maintenance in order to keep the database files from growing excessively large.

6.5.4 SETUP UPDATE

This option allows the CMCC Officer to change information regarding the account that was originally entered during the installation process. This option can update such items as a new CMCC Officer, a unit redesignation, change of zip code, etc.

6.5.5 EXIT

This option will exit and return to the Utilities Menu.

6.6 EXIT

Option 6 or X from the Utilities Menu will exit and return to the Main Menu.

SECTION 7. EXIT

7.0 EXIT MENU

Option 7 or X from the Main Menu will exit and return to operator to the logon screen. At this point, the current user is "logged off" for accountability purposes and the computer can be left on waiting for the next user. Two options are available at this point: a new user may log on or the system can be shut down for the day.

7.1 LOGON NEW USER

Option 1 or L of the Exit Menu will permit a new user to log on to the COMMANDOC system. After any prior menus have been selected and exited, the COMMANDOC system should remain at this position. This option should then be selected whenever additional actions are required. An operator's time on the system (as measured for the Usage Report) begins when he logs on to the system and ends when he exits back to the main menu.

7.2 QUIT FOR THE DAY

Option 2 or Q of the Exit Menu should be used at the end of each workday. This process is required for the system to properly close down and also enters into an automatic backup routine. This backup is an essential part of the integrity of the COMMANDOC system. See Section 8 for further discussion on backups.

SECTION 8. EMERGENCY BACKUP/RESTORE OF THE SYSTEM

1. General. The backup and restore process utilizes the MS-DOS BACKUP and RESTORE commands. Therefore, the computer's DOS subdirectory (containing the BACKUP and RESTORE commands) must be in the path statement in order for COMMANDOC to perform properly. If the backup process takes more than one disk, it is very important that the disks be numbered and entered in the proper sequence for a restore process.

2. Backup

a. *General*. The COMMANDOC system performs a backup operation every time the system is shut down for the day. This option completes the same cycle without shutting down the system. Follow the instructions provided on the screen. If the size of the database requires more than one disk for the backup process, it is very important that the disks be properly labeled and numbered.

b. *Procedure*. A three cycle backup process is recommended where day one's backup becomes the disk for day four; day two's disk for day five; and days three disk for day six. This is referred to as a grandfather-father-son system. This provides three backups, each one one day older than the one before it. Backup disks should be kept separate from the computer they belong to. In the event of theft of natural disaster, the same threat that takes the

computer will probably take the backup disk if it is in the same proximity.

2. Restore. Take the following steps to restore the COMMANDOC system and databases.

-Ensure that the computer is properly running and is set to the COMMANDO subdirectory.

-Insert the backup disk (or the first of the series if more than one) into drive A and type "RESTORE A: C:/S".

-Follow the instructions on the screen, replacing disks as necessary.

LIST OF REFERENCES

CSC-STD-002-85, Department of Defense Password Management Guideline, Computer Security Center, Fort George G. Meade, MD, 12 Apr 1985.

Kroenke, David M. and Kathleen A. Dolan. Database Processing Fundamentals-Design-Implementation. Chicago: Science Research Associates, Inc., 1988.

MCO P1080.20H, Joint Uniform Military Pay System/Manpower Management System Codes Manual (JUMPS/MMS CODESMAN). Washington, DC: 22 Dec 1981.

Olympia, P. L. and Kathy Cea. Developing FoxPro Applications. Reading: Addison-Wesley, 1990.

OPNAVINST 5510.1H, Department of the Navy Information and Personnel Security Program Regulation. Washington, DC: 29 Apr 1988.

SECNAVINST 5239.2, Department of the Navy Automated Information Systems (AIS) Security Program. Washington, DC: 15 Nov 1989.

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Commandant of the Marine Corps Code TE 06 Headquarters, U. S. Marine Corps Washington, D. C. 20380-0001	1
3.	Library, Code 52 Naval Postgraduate School Monterey, California 93943-5002	2
4.	Professor Myung W. Suh, Code AA/SU Naval Postgraduate School Monterey, California 93943-5002	1
5.	Professor Magdi Kamel, Code AA/KA Naval Postgraduate School Monterey, California 92943-5002	1
6.	Major Terrance C. Brady, USMC USTRANSCOM TCJ6-DA Scott AFB, Illinois 62225-7001	2