U.S. Marine Corps

DATA ACCESS SECURITY

PCN 186 523906 00

DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
WASHINGTON, D.C. 20380-0001

IN REPLY REFER TO

5239/06
CCIS-30
MAR 2 8 1990

From: Commandant of the Marine Corps

Subj: DATA ACCESS SECURITY

Ref: (a) MCO P5510.14
(b) DAS PLAN OF 10 MAY 85
(c) MCO 5271.1

Encl: (1) IRM-5239-06

1. PURPOSE. To provide further guidance and procedures on the implementation and maintenance of data access security contained in references (a) and (b) for functional managers sponsoring Automated Information Systems (AISs), field commands accessing the AISs and Automated Data Processing (ADP) sites storing AIS data.

2. AUTHORITY. This publication is published under the authority of reference (c).

3. APPLICABILITY. The guidance and security standards contained within this technical publication apply to all Marine Corps activities, personnel, and contractors who have access to the Marine Corps Data Network (MCDN). Activity Directors, as custodians of ADP resources will not allow access to stored information until the requirements of this standard are met. This standard is applicable to the Marine Corps Reserve.

4. SCOPE.

a. Compliance. Compliance with the provisions of this publication is required unless a specific waiver is authorized.

b. Waivers. Waivers to the provisions of this publication will be authorized only by CMC (CC) on a case by case basis.

5. RECOMMENDATIONS. Recommendations concerning the contents of this technical publication should be forwarded to CMC (CCI) via the appropriate chain of command. All recommended changes will be reviewed upon receipt and implemented if appropriate.

5239/06
CCIS-30

Subj: DATA ACCESS SECURITY

6. SPONSOR. The sponsor of this technical publication is CMC (CCI).

G. L. McKAY
By direction

DISTRIBUTION: PCN 186 523906-00

Copy to: 8145001

UNITED STATES MARINE CORPS

Information Resources Management (IRM)
Standards and Guidelines Program

DATA ACCESS SECURITY
IRM-5239-06

Enclosure (1)

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Received	Date Entered	Signature of Person Entering Change

PUBLICATION TABLE OF CONTENTS

LIST OF FIGURES

Chapter Table of Contents

Chapter 1

GENERAL

Chapter 1

INTRODUCTION

1.1. PURPOSE. This technical publication provides guidance and information on the background, policies, and applications for implementing and maintaining Data Access Security within the Marine Corps Data Network (MCDN). The typical audience for this technical publication is the Automated Data Processing (ADP) activity's Computer Systems Security Officer (CSSO) and his/her Central Security Control Administrator (SCA). This document provides guidance on implementing policy set forth in MCO P5510.14.

1.2. BACKGROUND

a. MCDN is a common-user, data communications network which provides terminal-to-computer and computer-to-computer communications access for all functional Marine Corps Automated Information Systems (AISs) for supporting establishment and Fleet Marine Force (FMF) units in built up areas. Any terminal connected to MCDN may be given access to these functional computers and the network in order to access the functional AISs required Input/Output (I/O) functions.

b. The Commandant of the Marine Corps (CCI) has established the software products CA-TOP Secret (TSS) and Natural Security (NSS) as the standard Marine Corps software security and access control products for mainframe computers connected to MCDN. CA-TOP Secret is a commercial product name; it in no way implies that it is classified in a military or national security sense. Due to the confusion that may result from referring to a security product as CA-Top Secret the Marine Corps has adopted TSS as its standard abbreviation. This technical publication will hereafter only refer to this security product as TSS.

c. The guidance and standards contained herein are intended to prevent unauthorized access, preclude unauthorized modifications, and prevent accidental or deliberate destruction and/or disclosure of Marine Corps data contained within MCDN.

d. The guidance and standards contained herein that pertain to TSS are based on Version 4.1 of TSS.

1.3. INFORMATION

a. The Marine Corps ADP Security Program has been established in recognition of the growing dependence upon interactive computer-based systems and the special problems involved in adequately securing these systems. As the data/information and the processing functions of these systems

become more sensitive, the risk potential (of these systems and the ADP activities at which these systems are resident) is expected to increase.

b. The objective of the Marine Corps ADP Security Program is to achieve the most effective and economical security posture. Attainment of this objective requires a balanced combination of staff and field actions to develop and implement proper policies and guidance, identify problems, requirements, and the solutions, and to adequately plan, program and budget for the resources required to implement an effective program.

c. The guidance and standards for ADP data security contained in this technical publication applies specifically to host computers within MCDN. Excluded from this plan is data/information embedded in microcomputer systems and tactical/combat weapons systems.

1.4. GUIDELINES

a. Data/information is entrusted to the custody of functional managers. It is the functional managers' responsibility to ensure the integrity of this data, the integrity of the information produced by their sponsored AISs and to grant and/or approve access to the data of which they are the functional manager. Appendix E contains a list of reference documents that address data access to functional manager AISs. Also refer to Data Security Administration Relationships (FIGURE B-03), User Access to a Local Node (FIGURE B-04), and User Access to a Remote Node (FIGURES B-05), in Appendix B.

b. The protection of information in a host computer system is the responsibility of the ADP activity responsible for the host computer system, until it is placed in the custody of another ADP activity or the end user. ADP activities which receive information from a host ADP activity must ensure the same level of protection is provided for the data received that was provided by the original host ADP activity. This protection responsibility includes providing a safe environment for the storage media, ensuring that all of the production systems' design integrity is maintained, as well as performing other custodial functions. Each ADP activity is responsible for the security of resources.

c. Protection of information, obtained from an ADP activity, by an NON-ADP activity, (e.g., printed information, information on a terminal screen, and information downloaded to a microcomputer or LAN), is the responsibility of the obtaining individual and the owner of the information. MCO P5510.14 applies.

d. Each user ID, (ACID), must correspond to one individual, or one type of Started Task. That is, there must be individual accountability for each user.

e. When TSS is nonfunctional, all access to resources must be terminated, other than access required to return TSS to a functional state.

f. TSS, NSS, ROSCOE, COMPLETE, and TSO internal security, vice JES, MVS, and COMTEN exits or modifications, will be used to implement security. Standards developed in conjunction with TSS apply to all other data security mechanisms whenever applicable. Applications requiring internal security will use TSS or NSS; waivers may be granted only by CMC (CCI). Proprietary software with internal security must conform to this requirement where feasible.

1.5. ORGANIZATION OF PUBLICATION. Chapters 1 and 2 relate to the overall view of ADP security within the Marine Corps. Each of the chapters following chapter 2 in this technical publication address the guidance and security standards associated with MVS or a specific software facility, provided it is managed by MVS (e.g., BATCH, TSO, ROSCOE, etc.).

Chapter Table of Contents

Chapter 2

ORGANIZATIONS AND RESPONSIBILITIES OF ADP SECURITY

Chapter 2

ORGANIZATIONS AND RESPONSIBILITIES OF ADP SECURITY

2.1. PURPOSE. The purpose of this chapter is to identify the organizational elements involved in implementing data/information access security and to outline their responsibilities.

2.2. ORGANIZATION. Six primary organizational elements are involved in the acquisition, delivery, installation, and maintenance of data/information access security: Headquarters Marine Corps (HQMC) C4 Division, Functional Managers, Systems Sponsor, ADP activities, Organization Heads, and MCCDPA, Quantico, Virginia. The actual administration of access security is performed by three types of security administrators: the Computer Systems Security Officer (CSSO) appointed by each ADP activity and the Terminal Area Security Officers (TASO) and TASO Administrators appointed by each organization head.

2.3. RESPONSIBILITIES

2.3.1. Director, C4 Division. The Director, Command, Control, Communications and Computer Division, (CMC CC) is the senior ADP policy official for the Marine Corps, and serves as the focal point for Marine Corps-wide policy, guidance and direction for the acquisition, operation, and overall management of all automated systems and resources. The Director, C4 Division is the Designated Approving Authority (DAA) regarding ADP security for the Marine Corps. Among the Director's responsibilities are:

a. Ensuring user compliance with ADP security directives promulgated by the DOD, Defense Intelligence Agency (DIA), National Security Agency (NSA), and Joint Chiefs of Staff (JCS).

b. Providing for the development, implementation, and maintenance of policies, guidance, procedures and standards appropriate to the management of the overall ADP security program.

c. Identifying ADP security related problems, requirements, and needs for resolution through use of acquisition and procurement actions.

d. Maintaining current knowledge in ADP system security and determining its applicability to ADP security problems, requirements, operations, and development efforts.

e. Managing the development, maintenance, and implementation of guidance relative to the physical, personnel, communications, emanations, hardware, software, procedural, and data security aspects of automated security with the advice and assistance of the offices identified herein as having collateral responsibility.

2.3.2. Functional Managers. Functional Managers will:

a. Formally appoint a system sponsor for each Automated Information System (AIS) under their cognizance.

b. Establish and publish policy governing user access authorization to AIS's under their cognizance. Policy will include requirements for down-loading of information to Personal Computers or Local Area Networks.

c. Ensure that systems under their cognizance are designed to include system security as a design objective in accordance with this technical publication, MCO P5510.14, MCO P5231.1, and other pertinent orders and regulations.

d. Functional managers of Class I systems and sponsors of Class II systems independent of Class I systems, are to formulate policy governing the authorization of access and administration of the data/information associated with the systems under their cognizance.

2.3.3. System Sponsors. System sponsors are responsible for Class I and Class II systems to be developed or currently operational. Persons so designated will:

a. Act as the focal point for all ADP security matters pertaining to the systems under their cognizance.

b. Identify and approve all controls and safeguards which regulate the manner in which sensitive data is processed and controlled in the systems under their cognizance.

c. Develop specific procedures for security testing and evaluation of the systems under their cognizance.

d. Provide assistance to CSSOs in evaluating the effectiveness of security controls and safeguards of the systems under their cognizance.

e. Conduct recurring review of test results of system security features at their respective ADP activity to ensure the maintenance of prescribed minimum security requirements.

f. Provide to the responsible system developers all security procedures and specification requirements pertinent to the systems under their cognizance.

g. Assist CSSOs in the resolution of any condition or activity which results in suspension or curtailment of the operations of the systems under their cognizance.

h. Sponsors of Class II systems dependent on Class I systems are to formulate policy governing the authorization of access and administration of the data associated with their systems.

i. Develop and field detailed security instructions with each class I/II AIS release.

2.3.4. Computer Systems Security Officer (CSSO). This billet was previously named the ADP Systems Security Officer (ADPSSO). The director of each ADP activity will appoint a CSSO who will:

a. Act as the focal point for, and principal advisor to the ADP activity director on all automated computer system security procedures, including personnel, physical security, communications, emanations, hardware, and software.

b. Be authorized to suspend operations partially or completely, immediately upon detection of activities which appear to compromise or jeopardize security. This authority shall allow suspension of support or service privileges to any system terminal subscriber, regardless of subordination, not adhering to regulations and procedures in effect at that time.

c. Report immediately to the ADP activity director any system failure leading to unauthorized disclosure, attempts to gain unauthorized access to sensitive information, or serious security deficiencies.

d. Inform, by message within 24 hours, to the Commandant of the Marine Corps (CCI), any occurrence where preliminary investigation appears to confirm a possible security violation which warrants HQMC awareness.

e. Ensure effective implementation of applicable ADP security regulations by:

(1) Preparing, disseminating, and maintaining plans, instructions, guidance and operating procedures required to ensure security of ADP operations.

(2) Conducting periodical surveys or reviews to determine compliance with such directives.

(3) Conducting formal reviews annually of threats and vulnerabilities so as to enable the ADP activity director to properly assess risks and determine effective measures to minimize such risks.

(4) Taking such measures as are appropriate to protect ADP activity assets from damage, destruction, alteration, or misappropriation.

(5) Continuously reviewing and evaluating the security impact of local computer systems changes, to include software/hardware interfaces, existing or proposed, with data communications or remote job entry (RJE) terminals.

(6) Coordinating and monitoring the conduct of periodic security indoctrination and training sessions for assigned personnel.

(7) Ensuring that audit trails are used effectively to provide for internal security audit and test, where warranted.

(8) Controlling and managing of all systems and user identifications and passwords.

(9) Perform periodic audits/reviews of the operating system for discrepancies in APF authorized libraries.

f. Ensures that all network and dial-up policies are enforced for the local node. Assists in maintaining overall network integrity by ensuring that accreditation requirements have been met prior to providing non CDPA/RASC equipment network access via the local node.

2.3.5. Organization Heads. Commanding generals/officers, and officers-in-charge of organizations will coordinate with their local ADP activity in the development of their respective commands' data security administration policy and structure per paragraph 2.3.2.d. They are responsible for system users within their organizations. This responsibility includes:

a. Ensuring that only those individuals with a need to know are granted access to ADP resources.

b. Ensuring that prior to issuing a user ID, each user is counseled concerning the responsibilities associated with their access privileges and the consequences of their abuse. Further they must ensure that each user has read and understands the Computer Fraud and Abuse Act of 1986, which is contained in Appendix D.

c. Appointing Terminal Area Security Officers. Terminal Area Security Officers must be appointed by each commanding general or officer, director, and officer-in-charge who has individuals in his/her organization with a requirement to use an AIS or MCDN.

2.3.6. Terminal Area Security Officer (TASO). TASOs are responsible for:

a. Ensuring local compliance with security operating procedures determined necessary in coordination with the CSSO of his local ADP site.

b. Ensuring that effective instructions specifying security requirements and operating procedures for the terminal area are issued.

c. Ensuring that each terminal user's need-to-know, level of clearance (where appropriate), and access authorizations are established commensurate with the data the user can obtain from terminals to which he is authorized access.

d. Managing the control and dissemination of user IDs and passwords.

e. Taking actions to assist the local ADP activity CSSO in ensuring overall system security.

f. Reporting to the CSSO of his local ADP activity, as soon as recognized, all practices inimical to overall systems security, and all instances of system security violations.

g. Assume responsibility for data obtained from the mainframe and "downloaded" to a Local Area Network (LAN) or Personal Computer (PC).

2.3.7. Directors of MCCDPAs and RASCs. Directors will:

a. Appoint the CSSO for their ADP activity.

b. Ensure that effective instructions specifying security requirements and operating procedures for the terminal area are issued.

c. Ensure that system sponsors of Class II systems are aware of this technical publication and of their responsibilities as established by this technical publication.

d. Be responsible for data access security training of TASO Administrators and TASO's as defined by this technical publication.

e. Ensure appropriate Log-on warning is provided as required by IRM 5239-08, Computer Security Procedures.

2.3.8. Director MCCDPA, Quantico. The Director will provide technical assistance to other ADP activities as required in support of this technical publication, and function as the TSS and NSS System Sponsor.

2.4. ADMINISTRATION. There are three primary administrative elements involved in the granting of access to data/information: (a) User Administration, (b) Functional Administration, and (c) Security Systems Administration.

2.4.1. User Administration

a. TASOs

(1) Scope of Responsibilities. Besides responsibilities

previously listed, the TASO will be the TSS Department Control Administrator (DCA) who will ensure:

(a) Every TASO must have access via a terminal to every ADP activity to which every one of the users he/she administers, has access.

(b) Every TASO must know of every user he/she administers. A TASO cannot ensure that access criteria is met and passwords are properly disseminated unless he/she knows the users he/she is to administer.

(c) Every TASO must have physical access to all spaces where his/her users gain access to MCDN.

(d) TASOs define their users to TSS and grant or gain them the appropriate access and authority required. These TASOs also gain NSS access for their users as required. Every user will be administered by the same TASO in both TSS and NSS at every ADP activity.

(2) Appointment. TASOs will be appointed in writing using the letter in FIGURE B-01, Appendix B. An information copy of the appointment letter must be forwarded to the TASOs and TASO Administrator. If the TASOs TSS Department is not in any TSS Division then the information copy of the appointment letter will be forwarded to the CSSO of each ADP activity where this TASOs TSS Department does not have a TSS Division. The original copy of appointment letter will be held by the appointing official after it has been endorsed by the appointee. TASOs will not be assigned by special orders. CSSOs of each ADP activity where this TASO has access to the ADP security system will be notified of the TASO appointment. The notification will include, but not be limited to, the following information about the TASO: 1) full name, 2) rank (if military) or grade (if civilian), 3) military ID or social security number, 4) work phone numbers, 5) mailing address, 6) TSS Department name and ACID, and 7) the TASO's ACID. Notification to a CSSO is not required if the TASO's TSS Department has a TSS Division, as the forwarding of the appointment letter in such cases will satisfy the requirement.

(3) Separation of Duties. TASOs who are also AIS users must separate their TASO duties. In these cases, the individual must be assigned two ACIDs, one for the performance of TASO duties and one for AIS functions. TASOs will, in general, assign and administer their own AIS user ACID.

b. TASO Administrators

(1) Scope of Responsibilities. Except in special cases, TASOs are grouped into divisions within their command structure. The administrators of a division (called TASO Administrators) must also be appointed by the commanding general, director, or

officer-in-charge of any organization who have individuals with a requirement to use MCDN. Besides the responsibilities listed above, TASO Administrators will be TSS Division Control Administrators (VCA) who will administer the TASOs within their division. TASO Administrators will also perform the duties of a TASO department administrator in the absence of TASOs to administer user's in any department within their division. This implies that:

(a) The TASO Administrator must have access via a terminal to every ADP activity to which the TASOs and users that are administered have access.

(b) Every TASO Administrator must know of every TASO he/she administers. A TASO Administrator cannot ensure that passwords are properly disseminated unless he/she knows the TASOs he/she is to administer. Each TSS Division must have at least two TASO Administrators appointed.

(c) TASO Administrators define their TASOs and users to TSS and grant or gain them the appropriate access and authority required. These TASO Administrators also gain NSS access for their TASOs as required. Every TASO will be administered by the same TASO Administrators in both TSS and NSS at every ADP activity.

(d) Every TASO Administrator must have access to all spaces where the TASO and users that are administered have access to MCDN.

(2) Appointment. TASO Administrators will be appointed in writing using the letter in FIGURE B-02, Appendix B. The original copy of appointing letter will be held by the appointing official after it has been endorsed by the appointee. TASO Administrators will not be assigned by special orders. CSSOs of each ADP activity where this TASO Administrator has access to the ADP security system will be notified of the TASO Administrator appointment. The notification will include, but not be limited to, the following information about the TASO Administrator: 1) full name, 2) rank (if military) or grade (if civilian), 3) military ID or social security number, 4) work phone numbers, 5) mailing address, 6) TSS Division name and ACID, and 7) TASO Administrator ACID.

(3) Separation of Duties. TASO Administrators who are also AIS users must separate their security duties from their users duties. In these cases, the individual must be assigned two ACIDs, one for the performance of his/her security functions and the other for the performance of his/her AIS functions. Refer to Data Security Administration Relationships, FIGURE B-03, in Appendix B.

c. System and Site Access. TASOs are responsible for obtaining AIS and site access for the users they administer.

TASO Administrator's are responsible for obtaining site access for the TASOs they administer. Access will be obtained as follows:

(1) Local Access to MCDN. Access to the MCDN Node to which the user's terminal is physically attached is obtained as described below. Once a user is defined to his/her local site, he gains access to additional resources from the resources' owner through his/her TASO. (See FIGURE B-04, User Access to a Local Node, in Appendix B.)

(a) The user must identify a requirement for access. In general, these requirements are placed upon a user by the sponsor of an AIS.

(b) The user's TASO must assign the user an ACID and ensure he/she has the appropriate access and authority. The procedures for gaining access to an AIS are defined by the system sponsor of the AIS.

(2) Remote Access. Before remote access is granted, local access must be first obtained as described above. Access to a site connected to the user's local site via MCDN is obtained as described below. Once a user is defined to the remote site, he gains access to additional resources from the resources' owner through his/her TASO, as in the case of local access. (See FIGURE B-05, User Access to a Remote Node, in Appendix B.)

(a) The user must identify a requirement for access based on a need-to-know basis. In general, these requirements are placed upon a user by the sponsor of an AIS.

(b) The user's TASO must assign the user an ACID and ensure he/she has the appropriate access and authority.

d. Password Control

(1) The issuance of a user ACID to an individual requires that the user's ACID password be protected from disclosure and to immediately change the password should it be compromised. The unauthorized and knowing disclosure of a password, or use of another individual's user ACID, are violations of the Computer Fraud and Abuse Act of 1986, Public Law 99-474, and may be punishable under Chapter 47 of Title 18 of the United States Code and under the Uniform Code of Military Justice.

(2) No one is to be permitted to look at, or list, passwords.

(3) Any TASO who needs to establish or reset a password will set it to a nontrivial, unique password, and set it to expire.

Chapter Table of Contents

Chapter 3

TSS ENVIRONMENT

Chapter 3

TSS ENVIRONMENT

3.1. PURPOSE. The purpose of this chapter is to identify the elements of the ADP security software product TSS as they apply to the ADP activity CSSO and his/her Central Security Control Administrators (SCA).

3.2. GENERAL OVERVIEW. TSS is designed to implement ADP security throughout the entire software community resident on an ADP activity's mainframe(s) by:

- Identifying users allowed to access the mainframe
- Controlling access to the operating system's facilities (e.g., BATCH, TSO, CICS, ROSCOE, etc.)
- Restricting access and use of ADP resources (e.g. data sets, programs, CICS transactions, etc.)

TSS is driven by MVS. By using the Standard Security Interface SU-32 or the System Authorization Facility (SAF) found in all versions of MVS, TSS accepts and validates all security checking requests issued by the security drivers inherent in major O/S components. CICS as do other IBM products along with many other vendor products also use SU-32. TSS is installed without any modifications to the operating system (RACF exit), therefore it is compatible with all software that utilize SU-32. The major components of TSS are its software logic and the files that this software accesses. Each of which will be expounded upon later in this chapter.

3.3. TSS FILES. TSS has five files which it may need to access: 1) Security File, 2) Backup Security File, 3) Parm File, 4) Audit File, and 5) Recovery File. Each of these files will be explained in the following paragraphs.

3.3.1. Security File. The Security File is in a BDAM data set format that contains at least four known segments: 1) ACID Segment, 2) Volume Segment, 3) Resource Segment, and 4) Dataset/Prefix Segment.

a. ACID Segment. The ACID Segment contains all ACID records utilized by the TSS software. The format of the records is an eight character key field with the remaining fields format known only to the vendor. The actual key, (ACID), may be from 1 to 8 characters long but where it is less than 8 characters the trailing spaces are part of the key. The standards for creating an ACID's key field, can be found in technical publication IRM-5234-04 (NAMING CONVENTIONS). The maximum for any one ACID record is 64K.

3.4. ACID HIERARCHY. The structure of the ACID Segment hierarchy can be broken down in to three types of records: 1) User, 2) Security File Administration, and 3) Profile.

3.4.1. User Type ACIDs. The User structure is the basic structure for defining a user ACID. There are three types of TSS ACIDs involved in this structure: 1) User ACID, 2) Department ACID, and 3) Division ACID.

a. A User ACID - The lowest level element in the ACID Segment organizational hierarchy. It is generally used to designate a specific person of a Department ACID or a Started Task's ACID. In fact, every User ACID must be associated with a single Department ACID. This User ACID is defined to the Security File by any type of Security File Administration ACID except another User ACID. With the exception of situations like terminals in the computer room running in support of console operations and ROSCOE, no ACID will be assigned for group use. Group ACIDs will be limited to specific terminals and must be explicitly authorized in writing by CMC (Code CCI). One of the users in the group must have their name appear in the name field of the security record associated with the group ACID. That individual will be held responsible for the use of the ACID, (e.g., in the case of an operational shift, the ACID should be assigned to the shift supervisor). Physical security is required for terminals accessed by group ACIDs in accordance with MCO P5510.14.

b. A Department ACID - TSS allows you to define multiple Department ACIDs within a Division ACID or a Department ACID need not be associated with any Division ACID. Defining a Department ACID without a Division ACID above it should be avoided when possible. Each Department is comprised of usually one or more User ACIDs. A Department ACID is defined to the Security File by any type of Security File Administration ACID above the level of a TSS Department ACID Administrator (DCA or TASO).

c. A Division ACID - TSS allows you to define multiple divisions within your ACID Segment structure. Each Division ACID is comprised of usually one or more Department ACIDs. A Division ACID is an Administration ACID above the level of a TSS Division ACID Administrator (VCA or TASO Administrator).

3.4.2. Security File Administration Type ACIDs. The Security File Administration structure is the structure for defining ACIDs that will enter TSS Security commands to modify the Security File. There are five types of TSS ACIDs involved in this structure: 1) User ACID, 2) Departmental control ACID (DCA or TASO), 3) Divisional control ACID (VCA or TASO Administrator), 4) Central Security Control ACID (SCA), and 5) Master Security Control ACID (MCA).

a. A User ACID - The lowest level in the Security File Administration ACID hierarchy. The scope of authority for a User

ACID is itself and therefore is not an Administrative ACID. This concept should not be overlooked and will be expounded upon in dealing with global profiles and Resource Owning ACIDs. This User ACID is the same type ACID previously described.

b. Department Administration ACID (DCA) - The scope of authority includes all ACIDs within the Department ACID that the DCA/TASO is owned by. This includes all User ACIDs, DCA/TASO ACIDs, Profile ACIDs, and resources owned within the Department ACID. There is one exception to this rule and that is a DCA/TASO can not create another DCA/TASO ACID. A DCA/TASO ACID is defined to the Security File by any type of Security File Administration ACID above the level of a DCA/TASO.

c. Division Administration ACID (VCA) - The scope of authority is all ACIDs within the Division ACID that the VCA/TASO Administrator is owned by. This includes all User ACIDs, DCA/TASO ACIDs, Department ACIDs, Profile ACIDs, VCA/TASO Administrator ACIDs, and resources owned within the Division ACID. There is one exception to this rule and that is a VCA/TASO cannot create another VCA/TASO Administrator ACID. A VCA/TASO Administrator ACID is defined to the Security File by any type of Security File Administration ACID above the level of a VCA/TASO Administrator.

d. Central Security Control ACID (SCA) - The scope of authority is all ACIDs within the Security File. This includes User ACIDs, DCA/TASO ACIDs, Department ACIDs, Profile ACIDs, VCA/TASO Administrator ACIDs, Division ACIDs, SCA ACIDs, and resources owned within the Security File. There is one exception to this rule and that is an SCA cannot create another SCA ACID. An SCA ACID is defined to the Security File by the MCA.

e. Master Security Control ACID (MCA) - The scope of authority is all ACIDs within the Security File. This includes all User ACIDs, DCA/TASO ACIDs, Department ACIDs, Profile ACIDs, VCA/TASO Administrator ACIDs, Division ACIDs, SCA ACIDs, and resources owned within the Security File. There is only one of these records within the Security file.

3.4.3. Profile Type ACID. The Profile structure is used when a group of Users or Administrator ACIDs need to use a set of identical resources or functions. It becomes convenient to define this set of access authorizations once and then associate the entire set to each of the User and/or Administrator ACIDs requiring the access. In TSS this set of common resource access characteristics is termed a Profile. Once a Profile ACID is defined it can be associated with any number of User and/or Administrator ACIDs, thereby eliminating the need to define each resource and resource access separately for every User and Administrator ACID. A Profile ACID can only be owned by a Department ACID; therefore, any Administrator ACID except a User

ACID may create a Profile ACID. There are two types of Profile ACIDs: 1) Conventional department Profile and 2) Global Profile.

a. A Conventional department Profile can only be attached to Users and/or Administrators ACID if both the User/Administrators ACID and the Profile ACID fall within the Administrator's scope.

b. A Global Profile may be added by any Administrator to any User/Administrator ACID within the Administrator's scope of authority.

3.4.4. Volume Segment. The format of the Volume Segment and the records contained in the segment are not supplied in the vendor's documentation. Based upon experienced TSS Administrators, the records contained in the Volume Segment of the Security File have a format of one record for every volume owned in the Security File and that each record contains the ACIDs to which the volume has been cross-authorized.

3.4.5. Resource Segment. The format of the Resource Segment and the records contained in the segment are not supplied in the vendor's documentation. Based upon experienced TSS Administrators, the records contained in the Resource Segment of the Security File have a format of one record for every resource owned, (other than Dataset/Prefix resources), in the Security File and that each record contains the ACIDs to which the resource has been cross-authorized.

3.4.6. Dataset/Prefix Segment. The format of the Dataset/Prefix Segment and the records contained in the segment are not supplied in the vendor's documentation. Based upon experienced TSS Administrators, the records contained in the Dataset/Prefix Segment of the Security File have a format of one record for every Dataset/Prefix owned in the Security File and that each record contains the ACIDs to which the Dataset/Prefix has been cross-authorized.

3.5. TSS FILES

3.5.1. Backup Security File. This is a data set that is not required for TSS to function. When utilized the format of the Backup Security File is identical to that of the Security File. If you utilize the Automatic Backup Option, (this option will be covered in Control Options under TSS SOFTWARE), or you issue the backup command, the Backup Security File will be a mirror image of the Security File at the completion of the backup process, and will remain that way until a TSS command is processed that updates the Security File. If DASD space permits this file should be utilized, but place it on a DASD volume other than where the Security File resides.

3.5.2. Parm File. This is the file that TSS reads, at startup time or any other time when TSS is taken down and brought back

back up, to obtain any modified Control Options other than the default options. All Control Options are covered in Appendix C.

3.5.3. Audit File. The Audit File is used to record security incidents. Violations and audited events are held in this wrap-around file; when the file is full, recording continues at the beginning of the file, overlaying existing data. Incidents can be generated by report or displayed online as the events occur. Use the vendor supplied program TSSUTIL to access this file for violation reports. The program TSSUTIL is contained in the vendor supplied manuals under REPORT AND TRACKING. Three years of audit information must be retained by each site.

3.5.4. Recovery File. The Recovery File records changes made to the Security File. It is a wrap-around file; when the file is full, recording continues at the beginning of the file, overlaying existing data. Should your Security File become unusable, the Recovery File records can be applied to the Backup Security file, with the vendor supplied program TSSRECVR. If used correctly your system down-time caused by an unusable Security File will be held to a minimum, (see vendor manual IMPLEMENTATION for complete instruction on Recovery Procedures). TSSRECVR must be owned by the MCA and access strictly controlled.

3.6. TSS SOFTWARE LOGIC

3.6.1. TSS Control Options. The Control Options at all ADP activities should be set to the same operand to minimize security software problems. The use of certain Control Options in the Parameter file should be avoided because experience has shown that they may cause problems. The available Control Options and the recommended usage in the Parameter File are specified in Appendix C.

3.6.2. Resources. The TSS is an access control software providing for the logical protection of resources at your ADP activity by:

- Identifying users allowed to use your system
- Controlling access to system facilities
- Protecting and insuring integrity of resources
- Restricting use of those resources

MVS directly requests validation of access to resources from TSS by means of the Standard MVS Security Interface. TSS validates access to the resource by examining access authorizations given to the user and returning an indication of whether to grant access to the resource or deny and fail the request. To access a given resource, a user must either own it, in which case he/she has full access, or must have been authorized by the owner for specific type(s) of access. If the access is not allowed, the

request is failed and a violation logged. TSS protects most resources by default. It also protects, by default, ACIDs, the element that identifies a user to TSS. Only those users whose ACIDs have been defined to TSS will be allowed to access the system. A positive definition is required first to access a system facility.

a. Assigning Resource Ownership. Assigning ownership of a resource or transferring the ownership from one ACID to another ACID will be the sole responsibility of the CSSO and his/her Central Security Administrators (SCAs). ACIDs other than the CSSO and his/her SCAs will not be authorized the administrative authority of OWN on any type of resource, but the assignment of resource ownership must be centrally controlled to ensure compliance with resource naming conventions and to prevent attempted duplication of ownership. The Profile ACID is not permitted to own resources. All other types of ACIDs may own resources. It is preferred that ownership be given to Division and Department ACIDs, but it is permissible for the MCA, SCAs, VCAs and DCAs to own resources.

3.6.3. ACID Definitions. The name field format for SCAs, VCAs, DCAs, and USERs, is Last name, First initial, Middle initial, rank for military or grade for civilians, if the ACID is not assigned, the name field will have the word VACANT in it and the ACID suspended. The Instdata field format for SCAs, VCAs, DCAs, and USERs, is AUTOVON phone number and/or commercial phone number, other information may be included in this field at the local site's discretion. A three character site ID should be included, in the INSTDATA field, for each additional site where the ACID has access. The name field in division and department ACIDs must contain the associated unit's name. Refer to IRM-5234-04 (Naming Conventions) for Naming Standards.

a. MCA Definition. The MCA will be defined only to the security systems that it administers. This account should not be utilized except when it is mandated that it must be used in order to perform those functions that only the MCA can perform. The MCA is assigned to the CSSO. The CSSO or Activity Director, may authorize the use of the MCA ACID by an SCA or other designated personnel to perform maintenance functions on the security file and other related TSS files.

b. SCA Definition. SCAs will be defined only to the security systems that it administers. Below are listed the maximum authorizations for an SCA.

(1) PASSWORD. The Password will expire at least every thirty days.

(2) LTIME (5). Terminal lock-time will never exceed five minutes, except as authorized by the CSSO in support of Auditing functions on a case by case basis and as a temporary lock time until such audits are complete.

(3) Administrative Authority

```
ACID (ALL)
DATA (ALL,PROFILE,PASSWORD)
FACILITY (ALL)
MISC1(ALL)
MISC9(TRACE,CONSOLE,MASTFAC,STC,GLOBAL,GENERIC,
 BYPASS)
RESOURCE(ALL)ACCESS(ALL)
```

c. Audit SCA Definition. A CSSO will have an Audit SCA ACID at all ADP activities were users that are within their sites's designator are administered. The maximum authorizations for an Audit SCA are:

(1) PASSWORD. The Password will expire at least every 30 days.

(2) LTIME(5). Terminal lock-time will never exceed 5 minutes.

(3) Administrative Authority

```
ACID (REPORT,INFO,AUDIT)
DATA(ALL,PROFILE,PASSWORD)
MISC9(GENERIC)
RESOURCE(REPORT,INFO,AUDIT)
DSN(AUDIT,REPORT,INFO)
```

(4) FACILITY(ROSCOE/CICS/TSO,BATCH)

d. VCA and DCA Definition. Each TSS division and department will have at least two administrators with identical maximum authorizations. The maximum authorizations for a VCA and DCA are:

(1) PASSWORD. The Password will expire at least every 30 days.

(2) LTIME(5). Terminal lock-time will never exceed 5 minutes.

(3) Administrative Authority

```
ACID(ALL)
DATA(ALL,PROFILE,PASSWORD)
MISC1(INSTDATA,SUSPEND)
MISC9(GENERIC)
RESOURCE(XAUTH,REPORT,INFO)ACCESS(ALL)
```

e. USER Definition. These are the ACIDs (or user IDs) used by end users to log onto a site's interactive facilities. If the user has the authority to submit batch jobs, this ACID will also

be used to initiate the user's batch sessions. The below sub-paragraphs are the maximum authorizations for a User.

(1) PASSWORD. The Password will expire at least every 90 days.

(2) LTIME(30). Terminal lock-time will never exceed 30 minutes.

(3) Administrative Authority - None.

f. Division, Department And Profile ACIDs Definition. Division, Department & Profile ACIDs are created as described in IRM-5234-04, Naming Conventions.

Chapter Table of Contents

Chapter 4

NSS ENVIRONMENT

Chapter 4

NSS ENVIRONMENT

4.1. PURPOSE. The purpose of this chapter is to identify the elements of the ADP security software product NSS as they apply to the ADP activity CSSO and his/her Central Security Control Administrators.

4.2. GENERAL OVERVIEW. NSS has been upgraded from 1.2 to 2.1. Guidance on the use and standards of version 2.1 will be provided at a later date.

Chapter Table of Contents

Chapter 5

MVS ENVIRONMENT

Chapter 5

MVS ENVIRONMENT

5.1. PURPOSE. The purpose of this chapter is to provide guidance and information on the Operating System software of MVS and how it should be defined in order to work with the ADP security software product TSS.

5.2. GENERAL OVERVIEW. TSS provides extensive and flexible security protection for resources maintained on your system. TSS uses the RACF exit of MVS to provide this authorization validation. TSS does not validate resources that are accessed by MVS for its own needs; therefore, the validation of MVS requires that MVS have regular security audits and that the resources that MVS is dependent upon are provided adequate security to ensure their integrity.

5.3. SYSTEM DATA SETS. In the following paragraphs if the data set is Write protected that means that writing to the data set should be restricted. If the data set is Read protected, that means reading the data set should be restricted.

5.3.1. Required By MVS IPL Volume

SYS1.NUCLEUS	WRITE PROTECT
SYS1.LOGREC	READ AND WRITE PROTECT
SYS1.SVCLIB	WRITE PROTECT

5.3.2. Required System Data Sets

SYS1.PARMLIB	READ AND WRITE PROTECT
SYS1.PROCLIB	WRITE PROTECT
SYS1.HASPACE	READ AND WRITE PROTECT
SYS1.HASPCKPT	READ AND WRITE PROTECT
SYS1.LPALIB	WRITE PROTECT
SYS1.LINKLIB	WRITE PROTECT
SYS1.DCMLIB	READ AND WRITE PROTECT
MASTER CATALOG	WRITE PROTECT
PAGE AND SWAP	READ AND WRITE PROTECT

5.3.3. Optional System Data Sets

SYS1.MANx	READ AND WRITE
SYS1.UADS	WRITE PROTECT
SYS1.CMDLIB	WRITE PROTECT
SYS1.VTAMLST	READ AND WRITE PROTECT
SYS1.VTAMOBJ	READ AND WRITE PROTECT
SYS1.VTAMLIB	WRITE PROTECT
SMP DATA SETS	WRITE PROTECT
JES PARAMETERS	READ AND WRITE PROTECT

SYS1.IMAGELIB	WRITE PROTECT
SYS1.DUMPxx	READ AND WRITE PROTECT
SYS1.MACLIB	WRITE PROTECT
DISTRIBUTION LIBRARIES	WRITE PROTECT

5.4. IPL OPTIONS. Control should be maintained for member IEASYS00 in SYS1.PARMLIB. Set option OPI, (allow operator override to IEASYS00), to OPI=NO. If the option is OPI=YES, then you need to ensure that the APF option is APF=00 and option LNK is LNK=(00,OPI=NO).

5.5. CONSOLE MESSAGES NOT DISPLAYED. To determine that the console messages not shown go to the IEASYS00 member of SYS1.PARMLIB, find option CMD. If the option is CMD=00 then look in member COMMND00 of SYS1.PARMLIB. In member CMMNDxx of SYS1.PARMLIB look for an entry of COM='SET MPF=xx', if the xx is 02, then member MPFLST02, (MPFLSTxx), on SYS1.PARMLIB contains the messages that are not displayed on the console.

5.6. PROGRAM FUNCTION KEYS (PFKs) WITH EMBEDDED PASSWORDS. To determine if there are embedded passwords in PFKs, go to the IEASYS00 member of SYS1.PARMLIB and find option CON. If this option is CON=(xx,L) where xx is 03, look at member CONSOL03 on SYS1.PARMLIB. In member CONSOL03, find the PFK entry. If the entry is PFK(xx) where xx is 01, look at member PFKTAB01 and (PFKTABxx) on SYS1.PARMLIB; it will contain the PFK setup. Look for the word "PASSWORD". Embedded passwords are considered internal security and must be removed.

5.7. AUTOERASE CONTROL OPTION. AUTOERASE controls the TSS Automatic Data Erasure feature. The use of this function is a requirement to maintain Class C2 functionality. The AUTOERASE control option operand must be set to YES when processing in a classified or controlled job environment. During a normal Day to Day processing environment, the operand will be set to NO to accommodate system performance and resources. DOD Directive 5200.28 has designated that all DOD systems will have Class C2 functionality (Controlled Access Protection) by 1992. Appropriate planning should be made by each site.

Chapter Table of Contents

Chapter 6

JES2 ENVIRONMENT

Chapter 6

JES2 ENVIRONMENT

6.1. PURPOSE. The purpose of this chapter is to provide guidance and information on the System software of JES2 and how it should be defined in order to work with the ADP security software product TSS.

6.2. GENERAL OVERVIEW. TSS provides extensive and flexible security protection for resources maintained on your system. TSS uses the RACF exit of MVS to provide this authorization validation. TSS does not validate resources that are accessed by JES2 for its own needs; therefore, the validation of JES2 requires that JES2 have regular security audits and that the resources that JES2 is dependent upon are provided adequate security to ensure their integrity. The JES Control option is only required if your site has modified the JCT, or desires support of the JES Early Password Verification Feature.

6.3. SYSTEM DATA SETS. Determining what level of access is required by all users can be difficult. In the following paragraph Write protected data sets means that writing to the data set should be restricted. If the data set is Read protected, reading the data set should be restricted.

6.3.1. JES2 Date Sets That Required Read/Write Protection.

SYS1.HASPACE	READ AND WRITE PROTECT
SYS1.HASPCKPT	READ AND WRITE PROTECT

6.3.2. HASPPARM Data Set. The name of this data set may be SYS1.PARMLIB; but to be certain, obtain the member name on this data set and list the proc called JES2 on SYS1.PROCLIB. There is a DD name of HASPPARM that points to the correct data set and the desired member name. This member will contain the JES2 Initialization Statements that should be audited.

Chapter Table of Contents

Chapter 7

BATCH ENVIRONMENT

Chapter 7

BATCH ENVIRONMENT

7.1. PURPOSE. The purpose of this chapter is to provide guidance and information on the Batch environment of MVS and how it should be defined within the ADP security software product TSS.

7.2. GENERAL OVERVIEW. TSS views Batch as just another facility which must be protected and authorized for use. To provide this protection each batch job must be associated with an ACID and a password so that TSS can determine which resources the batch job can access. To TSS, a batch job's ACID is exactly like a user ACID. It has an associated user record with a set of specific access authorizations. All system entry restrictions that can be designated for a user ACID are available for a batch job ACID (e.g., facility, source of origin, and CPU restriction).

7.3. PARM FILE ENTRIES. There are three Control Options in the Parm File that directly affect the facility of Batch.

7.3.1. JOBACID. The JOBACID control option identifies the field on every batch job card from which the ACID will be derived if no USER=field is present on the job card. The required operand is U,6. This operand indicates that when the job card is read by JES, it must have the USER=field.

7.3.2. SUBACID. The SUBACID control option indicates how TSS will derive an ACID for batch jobs that are submitted by the following methods: 1) through an online terminal, 2) from another batch job, and 3) from a started task. the required operand values are U,6. This operand indicates that the first six characters of the logged on user's ACID, or of the ACID associated with the Started Task, or Batch job will be used as the ACID for the submitted batch job provided there is no USER=field on the Job card.

7.3.3. Facility Operand WARNPW. The WARNPW operand forces defined users and jobs to use their correct passwords during the WARN mode. The default for the WARN mode would normally allow a job to process even if the user omitted his/her password or entered it incorrectly. It is recommended that the operand WARPW be placed on a Control Option record for Batch. (See example below.) This will offer some protection, if for some reason, an ADP activity should have to go from FAIL mode back to WARN mode for a temporary time frame.

```
FACILITY (BATCH=WARNPW)
```

7.4. TSS ABSTRACTS. There are two TSS ABSTRACTS that directly affect the facility of Batch.

7.4.1. JOBNAME. In order for an ACID to execute a batch job, the TSS Installation Exit requires that the ACID have access to an ABSTRACT whose first two characters are J#. The character(s), from 1 to 6 characters, that follow the J# must match the JOBNAME of the batch job, starting with the first character of the JOBNAME. For example, if an ACID has been permitted an ABSTRACT of J#T, then the ACID may execute with any JOBNAME provided that the first character of the JOBNAME begins with the character 'T'. If an ACID is only to be able to execute jobs that begin with TT7030, then the ACID would be permitted only one ABSTRACT that begins with J#, and the ABSTRACT would be J#TT7030.

7.4.2. JOB CLASSES. In order for an ACID to execute a batch job, the TSS Installation Exit requires that the ACID have access to an ABSTRACT whose first seven characters are CLASS##. The character that follows the CLASS## must match the JOB's CLASS< (CLASS=) of the batch job. For example, if an ACID has been permitted an ABSTRACT of CLASS##T, then the ACID may execute with a JOB CLASS OF T (CLASS=T).

7.5. BULK DATA ACIDS. Must have an associated non-expiring password at all sites. Refer to IRM-5234-04, Naming Conventions.

Chapter Table of Contents

Chapter 8

STARTED TASK COMMAND (STC) ENVIRONMENT

Chapter 8

STARTED TASK COMMAND (STC) ENVIRONMENT

8.1. PURPOSE. The purpose of this chapter is to provide guidance and information on the STC environment of MVS and how it should be defined within the ADP security software product TSS.

8.2. GENERAL OVERVIEW. STCs by default are not protected by TSS. To prevent security exposure, however, it is prudent to protect Started Tasks. Security protection for STCs is provided once they are defined to TSS.

8.3. STC ACID RECORD. Defining a Started Task to TSS, results in the association of the STC with a specific ACID or action or both. STCs are defined through the following operation:

```
TSS ADDTO(STC)PROC(stcname)ACID(acidname)
                    OR
TSS ADDTO(STC)PROC(stcname)ACID(acidname)STCACT
```

where: stcname is the name of the Started Task PROC name or the value of 'DEFAULT'. Use the value of 'DEFAULT' to set a default ACID or action.

acidname is a specific ACID or an action to be taken. The possible actions that may be specified are:

1) BYPASS - bypass security
2) UNDEF - treat as undefined user
3) FAIL - fail undefined STC
4) PROMPT - prompt the operator to supply an ACID and password

STCACT requests that the operator supply his/her operator ACID and password for STC accountability.

8.3.1. ACID STC Processing. The ACID that is associated with the STC, PROC, must be created with Facility 'STC' to allow execution as a Started Task. Do not specify any other facilities to ensure that the ACID is only used for the Started Task and cannot be executed otherwise.

8.3.2. DEFAULT STC Processing. The recommended method of processing DEFAULT is to fail the undefined STCs. To enter this option in the STC ACID, enter the following TSS command:

```
TSS ADD(STC)PROC(DEFAULT)ACID(FAIL)
```

8.3.3. ACID/Password Prompting STC Processing. With this method, personnel are allowed to use their own started tasks by

creating STC/ACID definitions that require the user to supply his/her own ACID and password. The STC will then execute under the authorizations provided for that user's ACID. A job submission procedure, for example, can be provided that is basically a shell that is missing authorization. The user's own ACID provides the authorization. To provide this option for Started Tasks, enter the following TSS Command:

```
TSS ADD(STC)PROC(stcname)ACID(PROMPT)
```

When an individual starts this STC, he/she will be prompted for his/her ACID and correct password. If an undefined ACID or an incorrect password is used then the STC will be failed immediately. The ACID that is entered must have access to the Facility of STC.

8.3.4. Individual Accountability STC Processing. To provide individual accountability, TSS allows the administrator to force an audit trail for sensitive and critical started tasks. Accountability forces the user to enter his/her ACID and correct password before allowing the started task to execute. If either the ACID or password is incorrect, the STC will fail to start. NOTE: The user's ACID is not used to control the execution of the Started Task (as in the method stated in paragraph 8.3.3 above); it merely indicates who replied to the prompt, provided that the individual takes care to protect his/her ACID's password. To force use of STC accountability, incorporate the STCACT keyword on any TSS ADD command to the STC ACID, for example:

```
TSS ADD(STC)PROC(stcname)ACID(acidname)STCACT
```

This is the standard way to add STCs (with the STCSCT option). Any STC entry which does not have this option should be issued a written waiver by the CSSO and appropriately audited.

8.3.5. STC Update Authority. Only the CSSO and Central Security Control Administrators should be granted the authority to update the STC ACID. The authority to update the STC ACID is granted to those ACIDs that have Administration of MISC9 option STC. Once MISC9(STC) is added update authority is permitted.

8.3.6. STC For Facilities. STCs that execute as facilities (ROSCOE, CICS, TSO, etc.) should have an ACID associated to them whose password had the option of NOPW.

8.4. TSS'S STCS. The STC that starts TSS must begin with the first three characters of 'TSS'.

8.5. Development/Test Environments. To ensure functionality within the production environment, all STCs should be defined as Fail and be given individual accountability via the STCACT option.

TSO ENVIRONMENT

Chapter 9

TSO ENVIRONMENT

9.1. PURPOSE. The purpose of this chapter is to provide guidance and information on the TSO environment of MVS and how it should be defined within the ADP security software product TSS.

9.2. GENERAL OVERVIEW. There are no special requirements for normal TSO operation with TSS. A TSO user must be defined to the TSO Table using TSO ACCOUNT.

9.3. PARM FILE ENTRIES. There is only one Control Option in the Parm File that directly effects the facility of TSO, as shown below.

FACILITY(TSO=PROMPT,NORNDPW)

9.3.1. Facility Operand PROMPT. PROMPT prevents a user from entering his/her password with his/her ACID when logging on, thus preventing the display of passwords on the screen. If a user enters the ACID and password at the same time, TSS will issue a warning message and lock the user's terminal for 10 seconds, then prompt for the password.

9.3.2. Facility Operand NORNDPW. NORNDPW cancels the random password operand which is the default operand in the Facilities Matrix for the Facility of TSO.

9.3.3. Facility Operand WARNPW. The WARNPW operand forces defined users to use their correct passwords during the WARN mode. The default for the WARN mode would normally allow a user to sign-on to TSO, even if the user omitted his/her password or entered it incorrectly. This offers some protection, if for some reason your ADP activity should have to go from FAIL mode to WARN mode for a temporary time frame. This operand is a default operand in the Facilities Matrix for the Facility of TSO; therefore, IT NEED NOT BE ENTERED IN THE FACILITY OPTION OF THE PARM FILE.

9.4. ACID ASSIGNED TO TSO'S STC. The ACID assigned to TSO's STC should be given the following:

a. Facility of STC only

b. Permitted DSN(*.)ACCESS(ALL)

c. PASSWORD(NOPW,0)

9.5. OWNERSHIP OF PROGRAMS. By default, users defined to the TSO facility will have access to all TSO commands and programs until restrictions are placed on an individual or group of users. TSS provides three methods for protecting TSO commands or command

subsets: 1) Protect all TSO commands using FACILITY(TSO=XDEF) in the Parm File, 2) Use the Limited Command Facility (LCF) to restrict use of special TSO commands, or 3) Protect TSO Commands as PROGRAMS. If you wish to own a program or a prefix of a program for the protection of the program or a group of programs utilized in the Facility of Batch, these programs/TSO commands will also become owned and, therefore, you will have to permit these TSO commands to the TSO users.

9.6. SIGN-ON SECURITY. Users must sign-on to TSO with their TSS ACID and password. Each user's ACID must be defined to the TSO.SYS1.UADS userid DATA SET. No password definitions are required on this file.

Chapter Table of Contents

Chapter 10

CICS ENVIRONMENT

Chapter 10

CICS ENVIRONMENT

10.1. PURPOSE. The purpose of this chapter is to provide guidance and information on the CICS environment of MVS and definitions within the ADP security software product TSS.

10.2. GENERAL OVERVIEW. TSS provides extensive and flexible security protection for CICS resources. No modification of CICS code is required to implement TSS security support.

10.3. PARM FILE ENTRIES. TSS comes with CICSPROD and CICSTEST already defined in the Facilities Matrix. There are two operands of Control Option FACILITY that are required and a third operand that may be required to make the Facility of CICS work correctly, as follows:

FACILITY(CICSPROD=NORNDPW,TYPE=CICS)
OR
FACILITY(CICSPROD=NORNDPW,TYPE=CICS,MRO)

10.3.1. Facility Operand NORNDPW. The Operand NORNDPW of the Control Option FACILITY in the Parm File cancels the random password operand which is the default operand in the Facilities Matrix for the Facilities of CICSPROD and CICSTEST.

10.3.2. Facility Operand TYPE=CICS. The operand TYPE=CICS must be specified in all Facilities Matrix entries that define a CICS Facility. The defined entries of CICSPROD and CICSTEST do not contain this operand.

10.3.3. Facility Operand MRO. The operand MRO must be specified in all Facilities Matrix entries that define a CICS Facility that is to execute in a MRO environment. A MRO environment utilities security records CSA to support multiple address spaces as one facility. The defined entries of CICSPROD and CICSTEST contain the operand of NOMRO.

10.3.4. Facility Operand WARNPW. The WARNPW operand forces defined users to use their correct passwords during the WARN mode. The default for the WARN mode would normally allow a user to sign-on to CICS, even if the user omitted his/her password or entered it incorrectly. This will offer protection if your ADP activity should have to go from FAIL mode back to WARN mode for a temporary time frame. This operand is a default operand in the Facilities Matrix for the Facility of CICS; therefore, IT NEED NOT BE ENTERED IN THE FACILITY OPTION OF THE PARM FILE.

10.4. ACID ASSIGNED TO CICS'S STC. The ACID assigned to CICS's STC should be given the following:

a. Facility of STC only

b. Bypassing of NOSUBCHK, NOVOLCHK and NORESCHK

c. PASSWORD(NOPW,0)

d. For ACIDs whose STC will be executing in a MRO environment, the ACID must have MRO added to it.

e. DSN *.,ACCESS(ALL)

10.5. CICS AND TSS INTERFACING. The principal areas in which TSS offers security protection for CICS are: 1) Sign-on security, 2) Password validation, 3) Terminal security, 4) Transaction security, 5) Resource level security (FCT, TST, DCT, JCT and PPT), 6) Terminal Locking, and 7) On-line TSS administration.

10.5.1. Multi-User Address Space. Under CICS each user signed on to the region, occupies part of the CICS address space. Consequently, when a user requests access to a resource, the operating system 'SEES' CICS performing the access--not the individual user. This process is typical of multi-user address spaces in general (e.g., ROSCOE, COMPLETE, etc.). Therefore, in order to protect resource accesses on the individual user level, CICS must issue its own security checks on behalf of the user performing the resource access. Since CICS performs these checks for all users within the address space, there is no reason for MVS to perform a duplicate check for CICS. As a result, the CICS address space is defined to TSS with the bypassing options as stated in paragraph 10.4. above.

10.5.2. Sign-On Security. Users must sign-on to CICS using their ACID and password. To sign-on, the user must be defined to TSS and authorized to access CICS. Automatic Terminal Sign-On may be used for terminals from which an explicit sign-on is not possible or not desirable. Automatic Terminal Sign-On is involved whenever a protected transaction is entered from a terminal for which no explicit sign-on has been performed. When this occurs, TSS will search its security file for an ACID which matches the terminal name. If the ACID is not found, the transaction will be failed and the user will receive message DFH3510, requesting the user to sign-on. If the ACID is found, then all of the normal security checking associated with this ACID will be performed with the exception of password checking. If the automatic sign-on is successful, the ACID will become associated with that terminal for that session just as if an explicit sign-on has been performed. Processing of the transactions intended will be initiated.

The ACID name generated will be as follows:

VTAM: the 8-character VTAM terminal name
TCAM: the 8-character TCAM terminal name
BTAM: the 4-character CICS terminal name

The installation selects which terminals are eligible for Automatic Terminal Sign-On simply by defining an ACID for those terminals. Since these ACIDs are in TSS terms, normal user ACIDs, security administration for these ACIDs is no different than other user ACIDs with the exception that the password given to the ACID is immaterial. The ACID should also be given a SOURCE which matches the terminal name, thereby preventing the ACID from being used from any other terminal. A possible use of this is in operations to permit the bringing down of CICS without having to sign-on to the CICS Facility.

10.5.3. CICS Resource Security. The Resources that should be protected are Transactions, FCTs and PPTs. Transactions should be protected through the use of OTRANS and not through the use of the Limited Command Facility (LCF). At a minimum, the permitting of OTRANS and PPTs should include the Facility pathing option. At a minimum, the permitting of FCT should include Facility pathing, Access pathing, and PRIVPGM pathing options. NEVER protect the sign-on transaction CSSN. If this transaction is protected, no one will be able to sign-on to CICS.

10.5.4. CICS Software Options. There are a number of options within CICS that the CICS Systems Programmer must specify. Ensure that the CICS Systems Programmer reads the vendor's manual, specifically the section titled INSTALLATION OF TSS (CA-TOP SECRET), WITH CICS.

10.5.5. Owned Transactions (OTRANS). All OTRANS used within CICS will be owned. Those OTRANS that require no restriction will be permitted to the TSS All record.

Chapter Table of Contents

Chapter 11

NCCF ENVIRONMENT

Chapter 11

NCCF ENVIRONMENT

11.1. PURPOSE. The purpose of this chapter is to provide guidance and information on the NCCF environment of MVS and how it should be defined within the ADP security software product TSS.

11.2. GENERAL OVERVIEW. TSS comes with NCCF already defined as a default facility in the Facilities Matrix. This means that the security attributes which control TSS processing for NCCF are predefined.

11.3. PARM FILE ENTRIES. There are no Control Options that need be defined in the Parm File for NCCF as the default values within the Facilities Matrix are sufficient.

11.3.1. Facility Operand WARNPW. The WARNPW operand forces defined users to use their correct passwords during the WARN mode. The default for the WARN mode would normally allow a user to sign-on to NCCF, even if the user omitted his/her password or entered it incorrectly. This will offer protection if your ADP activity should have to go from FAIL mode back to WARN mode for a temporary time frame. This operand is a default operand in the Facilities Matrix for the Facility of NCCF; therefore, IT NEED NOT BE ENTERED IN THE FACILITY OPTION OF THE PARM FILE.

11.4. ACID ASSIGNED TO NCCF'S STC. The ACID assigned to NCCF's STC should be given the following:

a. Facility of STC only

b. Permitted DSN(*.) ACCESS (ALL)

c. PASSWORD (NOPW,0)

11.5. NCCF SOFTWARE CONSIDERATIONS. NCCF must be generated with the option VERIFY=RACF.

11.6. NCCF AND TSS INTERFACING. All NCCF users must be defined to NCCF with dummy passwords. TSS validates facility access and password. There is no password change facility within NCCF requiring that expired passwords be changed manually by an Administrator. Facility and CPU checking is also performed.

Chapter Table of Contents

Chapter 12

ROSCOE ENVIRONMENT

Chapter 12

ROSCOE ENVIRONMENT

12.1. PURPOSE. The purpose of this chapter is to provide guidance and information on the ROSCOE environment of MVS and how it should be defined within the ADP security software product TSS.

12.2. GENERAL OVERVIEW. TSS provides extensive and flexible security protection for ROSCOE commands and monitors, and resources. ROSCOE versions beginning with Release 5.3 are fully supported. No modifications of ROSCOE code are required to implement TSS security support. The ROSCOE security exits provide the security support, and the vendor for TSS provides the code.

12.3. PARM FILE ENTRIES. TSS comes with ROSCOE already defined in the Facilities Matrix. There is one TSS control option and two operands of the Control Option that are required to make the Facility of ROSCOE work correctly.

12.3.1. Control Option DEFDSNPROT. The Control Option DEFDSNPROT must have operand 'NO' for exit DSAEXIT, to function correctly. This exit provides for OS data set validation.

12.3.2. Facility Operand NOLUMSG. The operand NOLUMSG of the Control Option Facility in the Parm File is required because the default of LUMSG in the Facilities Matrix causes ROSCOE to malfunction. The interface between ROSCOE and TSS that deals with this operand does not function correctly.

12.3.3. Facility Operand WARNPW. The WARNPW operand forces defined users to use their correct passwords during the WARN mode. The default for the WARN mode would normally allow a user to sign-on ROSCOE, even if the user omitted his/her password or entered it incorrectly. This will offer some protection if your ADP activity should have to go from FAIL mode back to WARN mode for a temporary time frame. This operand is a default operand in the Facilities Matrix for the Facility of ROSCOE; therefore, IT NEED NOT BE ENTERED IN THE FACILITY OPTION OF THE PARM FILE.

12.4. ACID ASSIGNED TO ROSCOE'S STC. The ACID assigned to ROSCOE's STC should be given the following:

a. Facility of STC only

b. Bypassing of NOSUBCHK, NOVOLCHK and NORESCHK

c. PASSWORD(NOPW,0)

12.5. ROSCOE AND TSS INTERFACING. The principal areas in which TSS offers security protection for ROSCOE are: 1) Sign-on

security, 2) Password validation, 3) Terminal security, 4) Command and monitor security, 5) Data set security via ZAP, UTILITY, IMPORT, EXPORT, 6) Job submission validation, 7) ROSCOE/ETSO security, 8) Output processor security, 9) Batch utilities protection, and 10) Administration security and gradual implementation of security mode.

12.5.1. Multi-User Address Space. Under ROSCOE, each user signed on to the region occupies part of the ROSCOE address space. Consequently, when a user requests access to a resource, the operating system 'SEES' ROSCOE performing the access--not the individual user. This process is typical of multi-user address spaces in general (e.g., CICS, COMPLETE, etc.). Therefore, in order to protect resource accesses on the individual user level, ROSCOE must issue its own security checks on behalf of the user performing the resource access. The vendor of TSS provided exits perform these security checks once they are linked into your ROSCOE Load Library. Since ROSCOE performs these checks for all users within the address space, there is no reason for MVS to perform a duplicate check for ROSCOE. As a result, the ROSCOE address space is defined to TSS with the bypassing options as stated in paragraph 12.4. above.

12.5.2. Sign-On Security. Users must sign-on to ROSCOE using their key and password. A user's key also becomes his/her ACID. By default, TSS recognizes the first 8 characters of the key as the ACID. To sign-on, the user must be defined to TSS and authorized to access ROSCOE. The user and his/her ACID must also be defined to the ROSCOE, ROSCOE ACCOUNT data set or USER PROFILE data set. As distributed by the vendor of TSS, once ROSCOE EXIT module ACFEXIT is installed and users change passwords, the ROSCOE ACCOUNT data set or USER PROFILE data set gets updated to reflect password changes.

12.5.3. Command and Monitor Security. The Limited Command Facility (LCF) can be used to restrict both commands and monitors, once the command exit (CMDEXIT) has been installed. LCF allows an inclusive list which specifies a list of commands and monitors the user is allowed, or an exclusive list which specifies a list of commands and monitors the user is not allowed. WARNING: The restricting of commands and monitors is very important.

12.5.4. Data Set Security. Anytime a user accesses an OS data set, the DSAEXIT is invoked. The DSAEXIT in turn issues a RECHECK which validates access to a data set. To accommodate the DSAEXIT, ensure that the TSS Control Option DEFDSNPROT of the Parm File has operand 'NO', as shown below.

```
DEFDSNPROT(NO)
```

The function of monitors ZAP, UTILITY, IMPORT, and EXPORT are validated on a data set access basis, and the user must have proper authority to access OS data sets. The following access

level authorizations are required in order to be authorized for the particular functions:

ZAP with REP or SETSSI requires UPDATE; otherwise READ
IMPORT requires READ authorization
EXPORT requires UPDATE authorization
UTILITY varies but UPDATE is common

12.5.5. Job Submission Validation. For jobs submitted through ROSCOE using the submit exit (SUBEXIT), TSS provides an additional security control feature beyond the basic batch job validation. This security feature determines whether the submitter has the authority to submit the job. In other words, TSS will check whether the ACID of the signed-on user is authorized to submit the ACID associated with the job via the USER= parameter on the job card. If he/she is not, the user will be notified that the job will be flushed at submission before the job is initiated. If the CMDEXIT is installed, the user will be notified that the job submission has failed.

12.5.6. ROSCOE Console Command. The ROSCOE Console Command should be restricted by local policy. The level of restriction is at the discretion of the local ADP activity.

Chapter Table of Contents

Chapter 13

COM-PLETE ENVIRONMENT

Chapter 13

COM-PLETE ENVIRONMENT

13.1. PURPOSE. The purpose of this chapter is to provide guidance and information on the COM-PLETE environment of MVS and how it should be defined within the ADP security software product TSS.

13.2. GENERAL OVERVIEW. TSS comes with COM-PLETE already defined as a default facility in the Facilities Matrix. This means that the security attributes which control TSS processing for COM-PLETE are predefined.

13.3. PARM FILE ENTRIES. There are no control Options that need be defined in the Parm File for COM-PLETE as the default values within the Facilities Matrix are sufficient.

13.3.1. Facility Operand ID. The default ID for COM-PLETE in the Facilities Matrix is the letter 'C'. The letter 'C' also is the default ID for CICSPROD in the Facilities Matrix. It is recommended that the ID for COM-PLETE be changed to the letter 'L' through the ID Operand of the FACILITY Option in the Parm File for COM-PLETE (as shown below). This will better identify the facility for violation reports.

```
FACILITY(COMPLETE=ID=L)
```

13.3.2. Facility Operand WARNPW. The WARNPW operand forces defined users to use their correct passwords during the WARN mode. The default for the WARN mode would normally allow a user to sign-on to COM-PLETE, even if the user omitted his/her password or entered it incorrectly. This will then offer some protection, if for some reason your ADP activity should have to go from FAIL mode back to WARN mode for a temporary time frame. This operand is a default operand in the Facilities Matrix for the Facility of COM-PLETE; therefore, IT NEED NOT BE ENTERED IN THE FACILITY OPTION OF THE PARM FILE.

13.4. ACID ASSIGNED TO COM-PLETE'S STC. The ACID assigned to COM-PLETE's STC should be given the following:

a. Facility of STC only

b. Permitted DSN(*.)ACCESS(ALL)

c. Permitted VOL(*ALL*)ACCESS(ALL)

d. PASSWORD(NOPW,0)

e. Bypass NOVOLCHK, NOSUBCHK

13.5. SIGN-ON SECURITY. Users must sign-on to COM-PLETE using their TSS ACID and password. User ACIDs must be defined to the COM-PLETE user maintenance file. Otherwise, the user will receive a message that userid is unknown.

Chapter Table of Contents

Chapter 14

CA-7/UCC7 ENVIRONMENT

Chapter 14

CA-7/UCC7 ENVIRONMENT

14.1. PURPOSE. The purpose of this chapter is to provide guidance and information on the CA-7/UCC7 environment of MVS and how it should be defined within the ADP security software product TSS.

14.2. GENERAL OVERVIEW. TSS comes with CA-7/UCC7 already defined as a default facility in the Facilities Matrix (it is defined with a name of UCC7). This means that the security attributes which control TSS processing for CA-7/UCC7 are predefined. It should be noted that personnel who have access to CA-7/UCC7 or have been cross-authorized the ACID of the STC for CA-7/UCC7 have access ALL to all data sets and volumes on the system. Close control must be maintained.

14.3. PARM FILE ENTRIES. There are no Control Options that need be defined in the Parm File for CA-7/UCC7 as the default values within the Facilities Matrix are sufficient.

14.3.1. Facility Operand WARNPW. The WARNPW operand forces defined users to use their correct passwords during the WARN mode. The default for the WARN mode would normally allow a user to sign-on to CA-7/UCC7, even if the user omitted his/her password or entered it incorrectly. This will offer protection if your ADP activity should have to go from FAIL mode back to WARN mode for a temporary time frame. This operand is a default operand in the Facilities Matrix for the Facility of CA-7/UCC7; therefore, IT NEED NOT BE ENTERED IN THE FACILITY OPTION OF THE PARM FILE.

14.4. ACID ASSIGNED TO CA-7'S/UCC7'S STC. The ACID assigned to CA-7's/UCC7's STC should be given the following.

14.4.1. Facility Of Batch, STC Only. This assumes that the batch jobs that are submitted by CA-7/UCC7 will not have an USER=Field in the Job Card; therefore, the ACID assigned to the STC of CA-7/UCC7 will be the ACID placed on the jobs submitted by CA-7/UCC7, as follows:

a. Permitted data sets of authorized jobs that are submitted by CA7.

b. PASSWORD(NOPW,0)

Note: Authorization to use CA-7 should not be permitted to personnel outside the ADP activity.

14.5. CA-7/UCC7 AND TSS INTERFACING. As this product is undergoing major modifications on its interfacing with TSS, you should consult the manuals provided by the vendor of TSS on this subject matter.

APPENDIX A

GLOSSARY

ACID: ACID is an acronym for "accessor ID." ACID refers to any named data structure in both the TSS and NSS security databases. ACIDs in TSS are: 1) MCAs, 2) SCAs, 3) VCAs, 4) DCAs, 5) users, 6) divisions, 7) departments, and 8) profiles. ACIDs in NSS are: 1) administrators, 2) persons, 3) groups, 4) members, 5) profiles, 6) applications or libraries, and 7) files. Interactive user ACIDs are commonly called, "user IDs." An ACID and the term "ACID" are integral parts of TOP SECRET.

Administrator ACID: An administrator's is an ACID which has ADP data security administrative authority.

ADP Activity: An ADP Activity is defined as a site operating under MVS with TSS installed and connected to the MCDN. The activities include MCCDPAs, RASCs, DFASCs, and ASCs. The term ADP Activity is also used to describe end user computing hardware that does not support MVS or TSS for the purposes of ADP accreditation and access controls.

ADPSSO: Each Marine Corps ADP site is required to appoint an ADPSSO. The exact duties of the ADPSSO are defined in MCO P5510.14. ADPSSOs are responsible for the effective implementation of ADP security regulations. These regulations are meant to ensure that the security needs of all functional sponsors are met and to resolve any conflicts between systems. Further they ensure that the ADP activities do not compromise their functional sponsor's data while acting as the sponsor's resource custodian. Recent changes in government directives revises this title to Computer Systems Security Officer (CSSO).

AIS: AIS is an acronym for "Automated Information System." SASSY, MIMMS, On-Line Diary, and ALPS are examples of AISs.

Application: An application is a NATURAL library used for the storage of NATURAL programs and source.

Authorized Program Facility: Authorized program facility (APF) is a facility in the MVS operating system used to designate programs which are authorized to run as if they are part of MVS. APF authorized programs rely almost entirely upon hardware to ensure that they do not destroy system integrity.

Batch ACID: A batch ACID is an ACID authorized to run only batch jobs.

Bulk Data Job: A bulk data job is a route execute job which uses a utility or special program. Features provided by bulk data not offered by strict route execute jobs include, data compression

(which facilitates fast transmission of the data) and check-pointing (which allows the job to be restarted should it be interrupted during a transmission).

Class I System: An AIS developed and managed by a functional manager at Headquarters Marine Corps for which the CMC (CC) provides technical support. Technical AIS support for the analysis, design, programming, and maintenance shall be provided by a Marine Corps Central Design and Programming Activity (MCCDPA), contractor, or as agreed to by the functional manager and the CMC (CC).

Class II System: An AIS under the functional control of an Headquarters Marine Corps staff agency, a FMF or supporting establishment organization for local use with technical support assigned to a command Information System Management Officer (ISMO) or a Regional Automated Service Center (RASC), or a Marine Corps Central Design and Programming Activity (MCCDPA).

Computer Systems Security Officer: See ADPSSO.

Data Definition Module: A data definition module is referred to as a file in NSS and is normally called a "user view" in data base terminology. User views are definitions of interfaces between user programs and database files (i.e., user views define how programs "see" data base files).

DCA: DCA is an acronym for "Department Security Administrator". A DCA is the lowest user organizational billet which administers resources. DCAs control access to data and facilities available on a host which belong to the department to which the DCA belongs. A DCA and the term "DCA" are integral parts of TOP SECRET.

Department: A department is the smallest ADP security entity used to define an ADP data security administrator's scope over ACIDs and resources. In TSS, a department is implemented as a department. In NSS, a department cannot be implemented. A department and the term "department" are integral parts of TOP SECRET.

Division: A division is a grouping of departments within a command or organization. In TSS, a division is implemented as a division. In NSS, a division cannot be implemented. Divisions own and control ACIDs, resources, and departments. A division and the term "division" are integral parts of TOP SECRET.

End User: See "System User".

Exit: An exit is an interface between a user program and the operating system.

Facility: A facility is a software resource which allows users access to a host. ROSCOE, COMPLETE, TSO, and JES are examples of

facilities. A facility and the term "facility" are integral parts of TOP SECRET.

Functional Manager: Functional managers are Headquarters staff agencies or field commands whose mission includes the management responsibility for a specific functional area such as: personnel, logistics, fiscal, intelligence, operations, or aviation.

Functional Support Goal: A functional support goal (FSG) is a service level agreement between CMC (CC) or an ADP activity and a system sponsor, functional manager, or a group of functional managers or system sponsors. The FSG defines each party's responsibilities in attaining mutually agreed upon ADP service levels.

Lock Time: Maximum period of time a user is allowed to be inactive before TSS locks the terminal.

MAF: MAF is an acronym for "Multiple Access Facility". This is a COMTEN software product which allows for application switching via the Basic Telecommunication Access Method (BTAM).

Mainframe: A mainframe computer is a large computer whose primary function is to run applications and utilities for data processing customers supporting a multiprocessing environment.

MCDN: MCDN is an acronym for "Marine Corps Data Network." MCDN not only allows computer to computer communications between these sites, but allows users terminal access to hosts at these sites.

MVS: MVS is one of IBM's standard operating systems. MVS is an acronym for "Multiple Virtual Storage".

NATURAL: NATURAL is a query language which allows interactive and batch access to the ADABAS data base. ADABAS is the Marine Corps standard database. "NATURAL" and "ADABAS" are registered trademarks of a Company named "Software AG".

NATURAL Security: NATURAL Security is an optional feature of NATURAL which provides security to NATURAL. NATURAL Security and TOP SECRET operate independent of each other and have no interface. "NATURAL Security" is a registered trademark of Software AG.

NSS: NSS is an acronym for "NATURAL Security".

Operating System: An operating system is software which controls the allocation and distribution of computer resources. It provides the interface to hardware for other software running on the computer.

Own/Owner/Ownership: The term own/owner/ownership, as used in the context of this technical publication, means primary

accountability for the data. It is not intended to convey a sense of personal property ownership, as that term is customarily used.

PCU: PCU is an acronym for "Production Control Unit." The unit is responsible for the scheduling, running and troubleshooting of production batch jobs.

Production Batch: Production batch is that group of Class I and II systems which are scheduled and run by the PCU at customers' requests.

Profile: A profile is a structure used to group authorizations to resources associated with common, specific functions. For example, a profile may contain all the authorizations required for a user of the DOV system to release batches. Rather than authorize each user to each resource required to release batches, each user could be attached to the "DOV releaser profile." This can be done with only one command per user; and once authorized to the profile, the user would obtain all of the authorizations contained within the profile. Profiles and the term "profile" are integral parts of TOP SECRET. In NSS, the term profile refers to a group.

Proprietary Software: Proprietary software is software purchased or leased from a software vendor for which CMC (CC) is the functional sponsor.

Resource: A resource is an entity protected from unauthorized access by a security system. In TSS, a resource is anything which can be administered and which is not an ACID. Data sets, abstracts, terminals, owned transactions, programs and CPUs are examples of resources in TSS. In NSS, NATURAL programs (in both source and object form), commands, transaction durations, and session parameters are examples of resources.

Route Execute Job: A route execute job uses Job Control Language (JCL) to send a job submitted at one node to another node for execution.

SCA: SCA is an acronym for "Central Security Administrator". This individual aids the MCA in the maintenance of TOP SECRET. An SCA and the term "SCA" are integral parts of TOP SECRET.

SMF: SMF is an acronym for System Maintenance Facility. SMF is an IBM facility used to record and monitor system events and performance.

System User: A system user is an organization or person having a valid requirement to use system capabilities.

Started Task: A started task is a TOP SECRET ACID assigned to a specific batch job or system. Tasks do not have interactive access. Execution JCL for tasks must be accessible to ADP site

personnel only (i.e., non-ADP site administrators may not create task ACIDs without the permission of the CSSO). Examples of tasks are: ROSCOE, COMPLETE, GTF, etc.

Terminal Area Security Officer (TASO): The head of every organization which receives service from a Marine Corps ADP activity is responsible for the appointment of a TASO. A TASO's responsibilities are defined in Chapter 2.3.6.

TOP SECRET: TOP SECRET is a product which provides host data security within IBM's MVS operating system. It interfaces with any IBM compatible product via standard IBM Resource Access Control Facility (RACF) exits.

TP Monitor: A TP monitor is an MVS task or job which manages interactive sessions. Examples of TP monitors are: ROSCOE, COMPLETE, TSO, CICS and NCCF.

TSS: TSS is an acronym for "TOP SECRET".

User ID: A user ID is an ACID assigned to an individual which allows interactive (i.e., on-line) access.

User Organization: See "System User."

VCA: VCA is an acronym for "Division Security Administrator". A VCA is the highest user organizational billet which administers resources. These resources belong to the division to which the VCA belongs. VCAs own and control DCAs. An VCA and the term "VCA" are integral parts of TOP SECRET.

VTAM: VTAM is an acronym for "Virtual Telecommunications Access Method." This is the IBM standard data communications software system designed to support networking.

APPENDIX B

APPOINTMENT LETTERS/USER ACCESS RULES

ORGANIZATION HEADING

5510
Code
Date

From: Organization Head
To: TASO's Name

Subj: APPOINTMENT AS TERMINAL AREA SECURITY OFFICER (TASO)

Ref: (a) MCO P5510.14
(b) IRM-5239-06 Data Access Security
(c) Computer Fraud and Abuse Act of 1986
(d) IRM-5239-07 Terminal Area Security Officer (TASO) Guide
(e) IRM-5234-04 Naming Conventions
(f) Notification Media to CSSOs

1. You are hereby appointed the TASO for (use the TSS Department ACID and its name). You are to thoroughly familiarize yourself with references (a) through (e). This appointment will remain in effect until you are formally relieved.

2. The CSSO's of the following ADP activities have been notified of this change of appointment via reference (f):

FIRST ENDORSEMENT

From: TASO's Name
To: Organization Head

Subj: TASO APPOINTMENT LETTER

1. I have read and understand references (a) through (e) and have assumed all duties in conjunction with my appointment to TASO.

FIGURE B-01
Example of TASO Appointment Letter

ORGANIZATION HEADING

5510
Code
Date

From: Organization Head
To: TASO Administrator's Name

Subj: APPOINTMENT AS TERMINAL AREA SECURITY OFFICER ADMINISTRATOR (TASO)

Ref: (a) MCO P5510.14
(b) IRM 5239-06 Data Access Security
(c) Computer Fraud and Abuse Act of 1986
(d) IRM-5239-07 Terminal Area Security Officer (TASO) Guide
(e) IRM-5234-04 Naming Conventions
(f) Notification Media to CSSOs

1. You are hereby appointed the TASO Administrator for (use the TSS Division ACID and its name). You are to thoroughly familiarize yourself with references (a) through (e). This appointment will remain in effect until you are formally relieved.

2. The CSSO's of the following ADP activities have been notified of this change of appointment via reference (f):

FIRST ENDORSEMENT

From: TASO Administrator's Name
To: Organization Head

Subj: TASO ADMINISTRATOR APPOINTMENT LETTER

1. I have read and understand references (a) through (e) and have assumed all duties in conjunction with my appointment to TASO Administrator.

FIGURE B-02
Example of TASO Administrator Appointment Letter

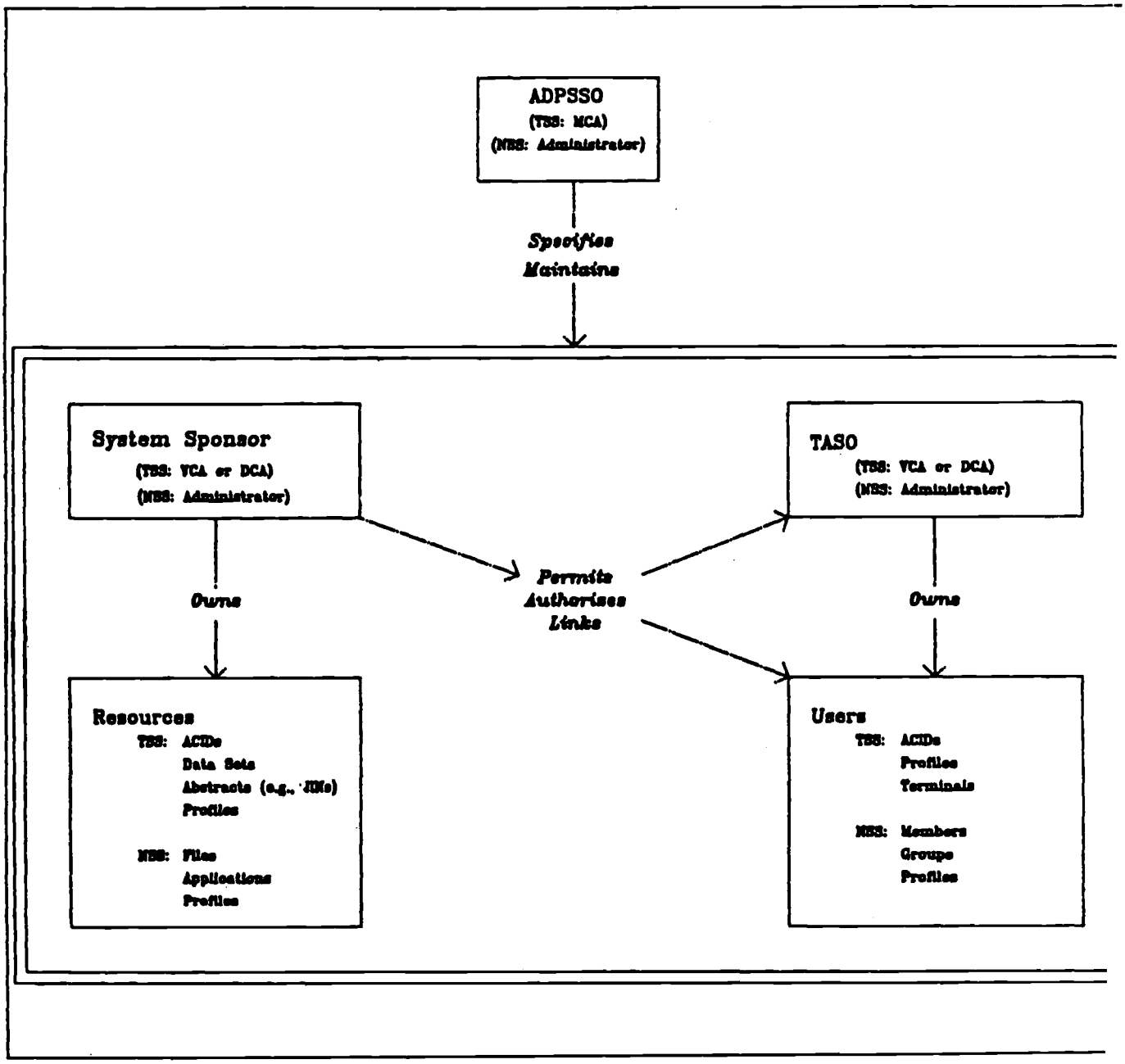

FIGURE B-03
Data Security Administration Relationships

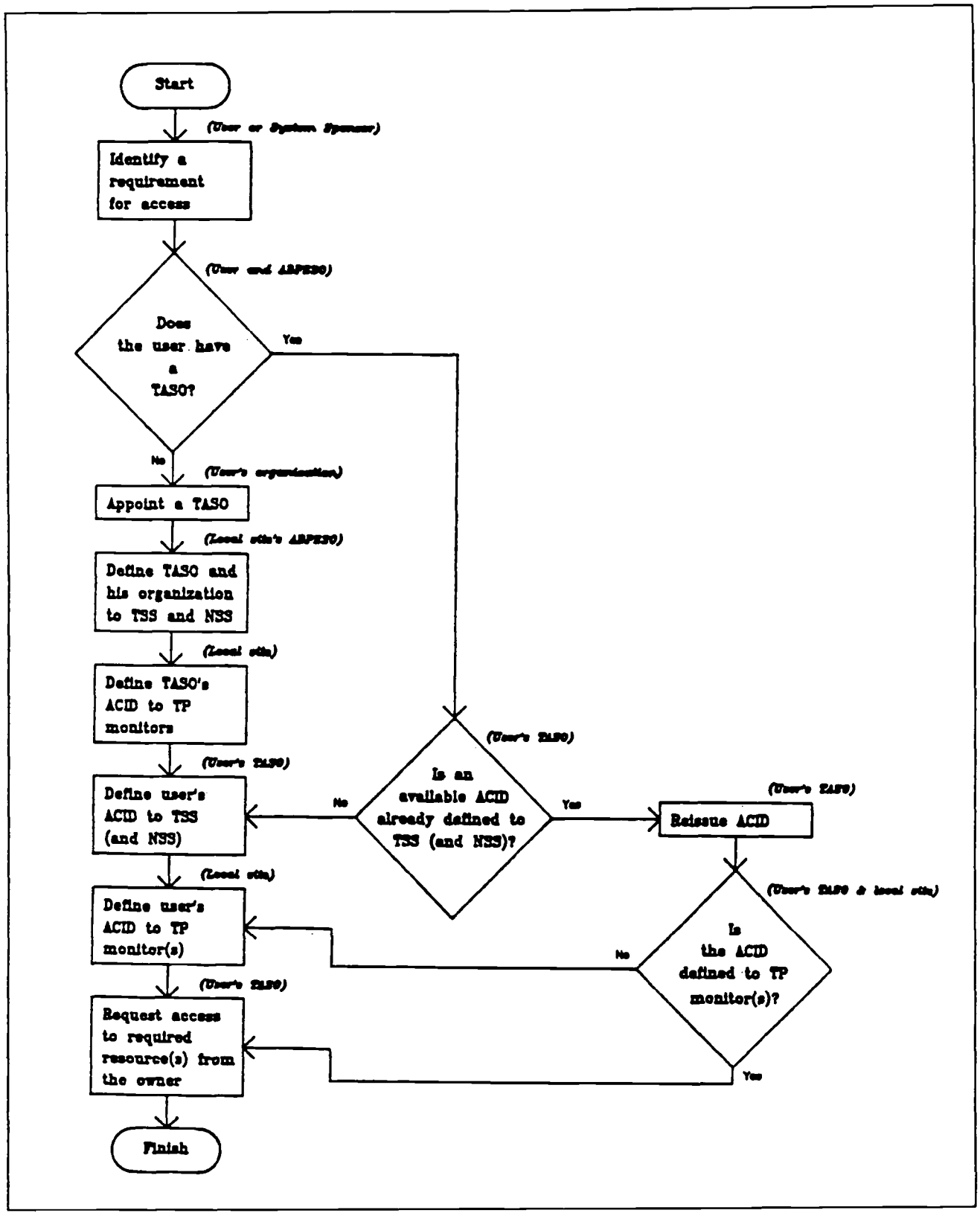

FIGURE B-04
User Access to a Local Node

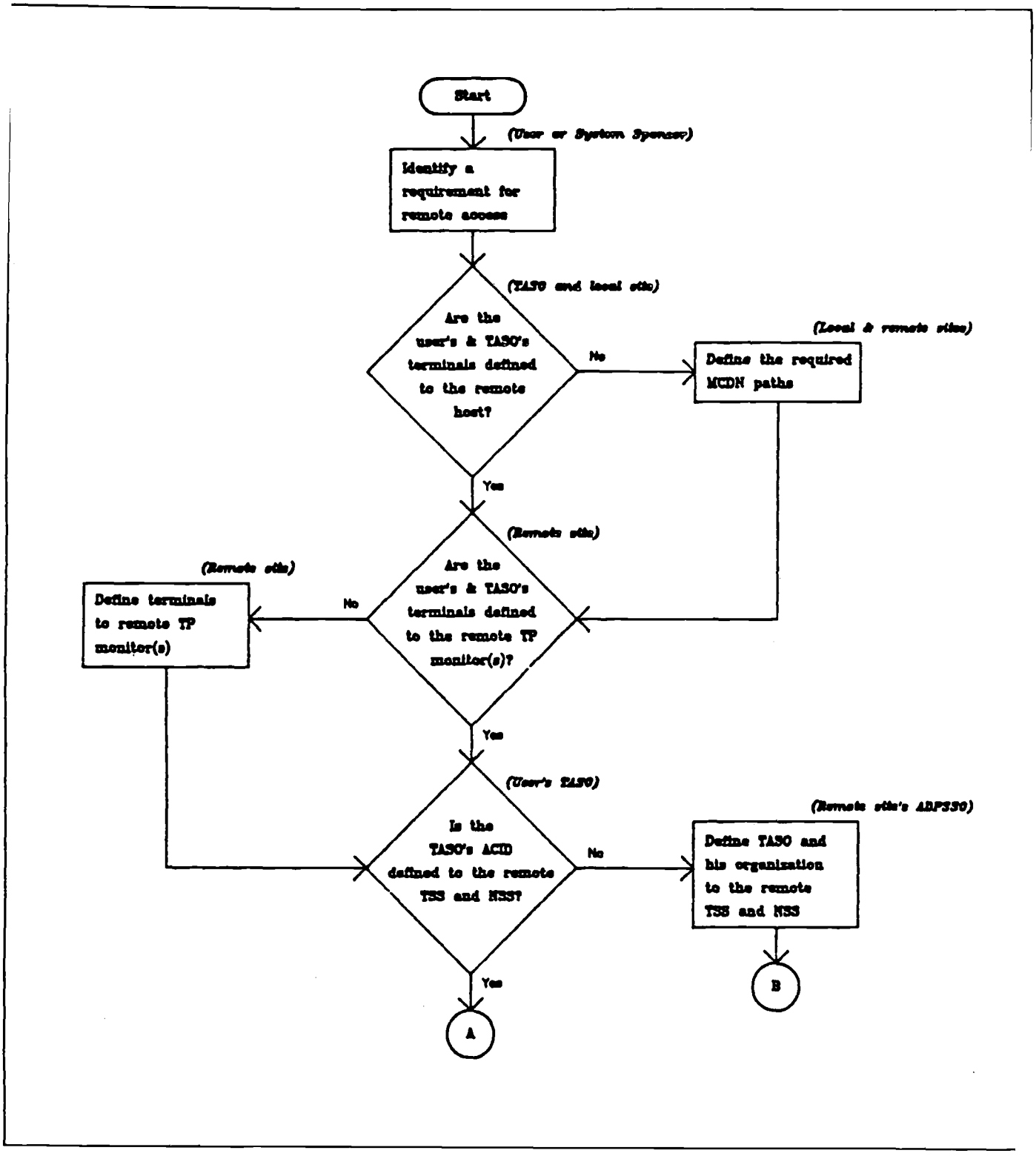

FIGURE B-05
User Access to a Remote Node (Page 1 of 2)

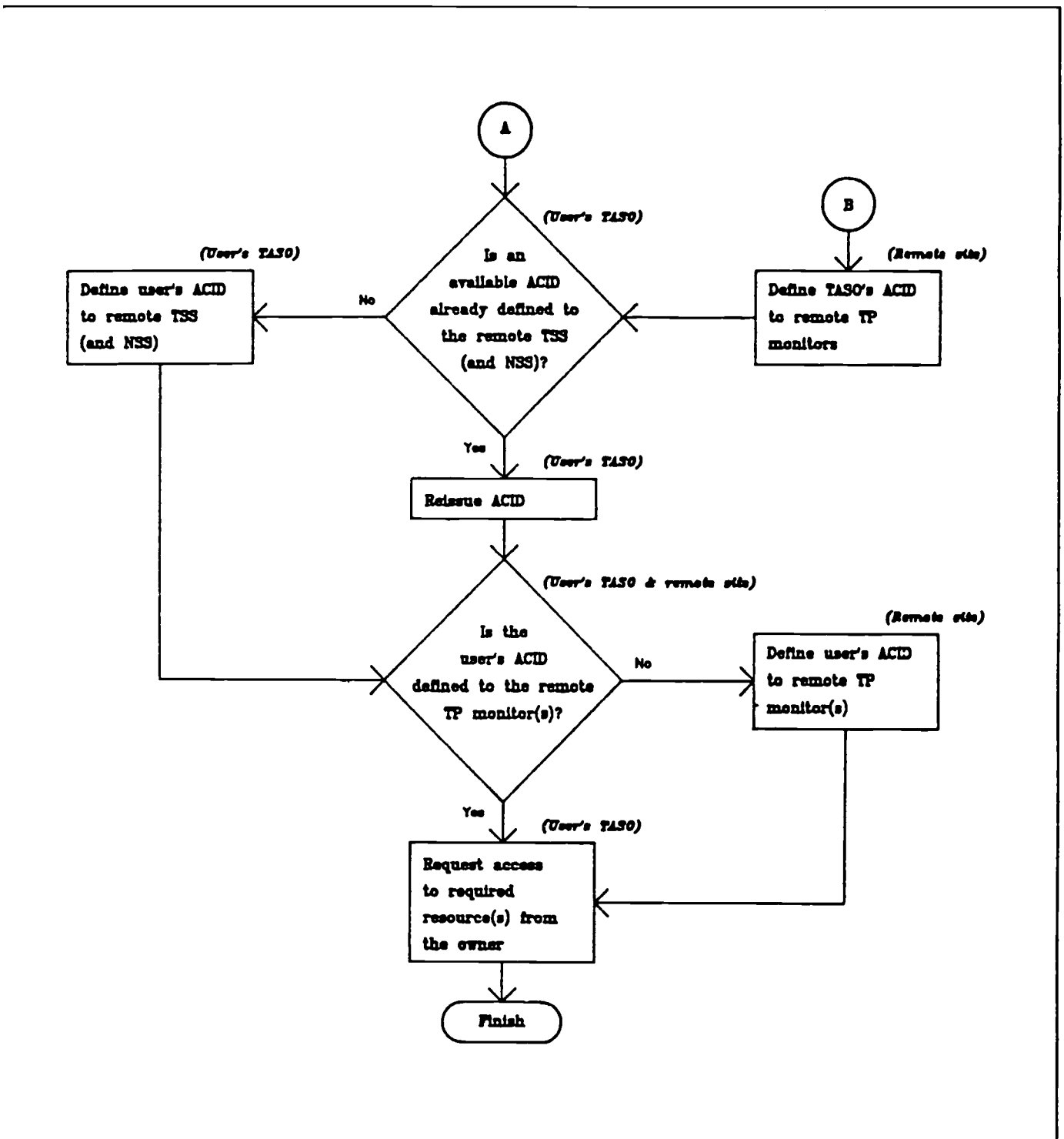

FIGURE B-05
User Access to a Remote Node (Page 2 of 2)

APPENDIX C

TSS CONTROL OPTIONS

Certain Command Options should not be specified in the Parm File because they may cause problems, as experience has shown. They should only be used during special situations, as recommended by the vendor. These commands are:

BYPASS
CANCEL
DIAGTRAP
DLIB - Used with a software package not maintained by the Marine Corps.
DUMP
REINIT
RESETEOD
RESETSTATS
ST
STATS
STATUS
SUSPEND
SYNCH
SYSOUT
TSS
VERSIONS
WHOOWNS

The recommended operands for those Command Options which may be used in Parm File are listed below:

ADSP - Automatic Data Set Protection allows the CSSO to determine which newly created data set will be automatically protected. The default is operand YES; it is recommended, but not required, that the operand of ALL be used.

AUTH - AUTH indicates whether TSS will merge the User ACID, Profile ACID(s), and the ALL ACID records for its access authorization search, or whether TSS will search each record separately. The DAS Plan of 10 May 1985 stated the default operand of OVERRIDE, ALLOVER would be used for this option. The use of program pathing with CICS has proven this operand to no longer be feasible. Therefore, it is required that all ADP activities use the operand of MERGE, ALLOVER. Before changing this operand, it is imperative that you contact MCCDPA, Quantico for assistance.

AUTOERASE - AUTOERASE controls the TSS Automatic Data Erasure feature. The use of this function is a requirement to maintain Class C2 functionality. The AUTOERASE control option operand must be set to YES when processing in a classified or controlled job environment. During a normal Day to Day processing environment, the operand will be set to NO to accommodate system performance and resources. DOD Directive 5200.28 has designated that all DOD systems will have Class C2 functionality (Controlled Access Protection) by 1992. Appropriate planning should be made by each site.

AVO - The AVO (Automatic Volume Ownership) option indicates if a scratch tape, which is undefined to TSS, will become automatically owned by the ACID running a job which keeps the scratch tape. The operand default of OFF is required for this option so that tape data sets are protected by DSN and not Volume.

BACKUP - The BACKUP option allows the CSSO to select a time for an automatic daily backup. It should be noted that at the time stated for this option, once TSS starts the backup process, it will not process any access request from the operating system until the backup process is completed. (For a Security File of 30,000 ACIDs, the backup process takes between 15 and 20 minutes.) You should pick a time of low on-line user activity.

BYPASS - Not valid for use.

CANCEL - Not valid for use.

DATE - This option specified the format for dates displayed in listings. The default operand of MM/DD/YY has been used since day one and is the recommended operand. Any ADP activity using a different format of DATE is required to notify all CSSOs of the different format.

DEBUG - DEBUG controls the production of debugging dumps used to determine the cause of abnormal error conditions. Normally the operand of OFF will be used.

DEFDSNPROT - Controls default protection of data sets in the WARN and IMPL modes. It is recommended that the operand of NO be used. The operand of 'NO' is required for proper DSN checking through the Facility of ROSCOE. (See Chapter 12, ROSCOE ENVIRONMENT.)

DEFPROT - Controls TSS default protection of all resources except data sets in all modes. It is recommended that the operand of NO be used. WARNING: If you use the operand YES, you must have ALL resources owned and permitted; this includes CPUs.

DIAGTRAP - Not valid for use.

DLIB - Not valid.

DOWN - This option identifies the type of job initiation, password changing, and AVO processing that TSS will perform when its address space is inactive. The required operands are BW,OW,SB,TW.

DUMP - Not valid for use.

EXIT - Activates and deactivates the installation exit. It is required that operand ON be used.

FACILITY - The FACILITY option controls the processing of each system facility or obtains the status of a facility. The following is the minimum that is required for each FACILITY along with the defaults for the FACILITY:

a. BATCH - FACILITY (BATCH=WARNPW)

b. STC - FACILITY (STC=WARNPW)

c. TSO - FACILITY (TSO=PROMPT,NORNDPW)

d. CICS - FACILITY(CICS=TYPE=CICSPRDD OR CICSTEST,NORDNPW)

e. ROSCOE - FACILITY(ROSCOE=NORNDPW,NOLUMSG)

f. COMPLETE - The Facility COMPLETE is valid only if PGM=THR. The newest version of COMPLETE, PGM=CAJ requires the use of of another facility (i.e., IDMSPROD=NAME=COMPLETE,PGM=CAJ).

Note: Do not use the facilities that begin with RESERV OR TONE.

HPBPW - The HPBPW option selects the maximum number of days that TSS will honor an expired or previous password for batch jobs. The required operand is 3.

INACTIVE - The INACTIVE option selects the number of days before TSS will deny an unused ACID access to the system after that ACID's password has expired. The required operand is 45.

INSTDATA - INSTDATA controls the value of the 8-byte global installation data area. This value is passed to the site security exit. The recommended operand is the default value of 0.

IOTRACE - controls a diagnostic trace for use by the vendor's technical support staff. The trace is produced on the TRACE/LOG data set. The recommended operand is OFF.

JES - The JES option is only required if the installation has modified the JES JCT control block or requires support for the JES Early Verify feature. The recommended operand is the default of NOVERIFY.

JOBACID - The JOBACID control option identifies the field on every batch job card from which the ACID will be derived if no USER=field is present on the job card. The required operand is U,6.

LOG - The option identifies the types of events that TSS will log and specifies whether the events will be logged onto the Audit Tracking File (ATF) and/or onto the System Management Facility (SMF). This option also specifies if the violation message will be displayed. The LOG option affects all facilities. This Global LOG command can, however, be overridden by a LOG operand entered as a suboption for a specific facility; therefore, THIS LOG OPTION WILL BE PLACED BEFORE ALL FACILITY OPTIONS WITHIN THE PARM FILE. The recommended operands are the default values of SMF,INIT,SEC9,MSG.

MODE - Selects the security mode in which TSS will operate for all facilities. The MODE option is used to set a global mode. Modes may also be assigned to a specific facility, or permitted to a specific ACID, therefore THIS MODE OPTION WILL BE PLACED BEFORE ALL FACILITY OPTIONS WITHIN THE PARM FILE. The required operand is the default value of FAIL.

MSUSPEND - Allows the MCA's ACID to be suspended automatically if the password violation threshold set via the PTHRESH option is exceeded. This will prevent a user from making an unlimited number of guess attempts to determine the MCA's password. The recommended operand is the default value of NO. Should you wish to use the value of YES, what are your options should this user who is attempting to sign-on to the MCA account also tried to sign-on to all of the SCA accounts and suspended all of them likewise.

NEWPW - NEWPW specifies the rules that TSS will apply when an ACID selects a new password. At a minimum, these operands are required: MIN=7,NR,ID,RS,WARN=7.

PTHRESH - This option limits the number of password violations a user may receive prior to his ACID being suspended. The required threshold is 4.

RECOVER - Indicates whether TSS will record changes made to the Security File onto the Recovery File. Changes include those made automatically by TSS and those made by TSS administrators via the TSS command. If you are using a Recovery File, the operand of ON is used.

REINIT - Not valid for use.

RESETEOD - Not valid for use.

RESETSTATS - Not valid for use.

RPW - The RPW control option allows the site to modify and list the contents of the Restricted Password list. This allows the site to prevent the use of obvious passwords such as MARINES. WARNING: Experience has shown that the use of comments (a space followed by an * and then a space and your comment) on this option is not valid and will cause a Parm File error when TSS is started. Experience has also shown less Parm File errors are encountered when these option records are the last records in the Parm File.

SECTRACE - SECTRACE activates a diagnostic trace on the activities of all defined users or of specific users. The recommended operand is the value of OFF.

ST - Not valid for use.

STATS - Not valid for use.

STATUS - Not valid for use.

SUBACID - The SUBACID control option indicates how TSS will derive an ACID from batch jobs that are submitted by the following methods: 1) through an on-line terminal, 2) from another batch job and 3) from a started task. The required operand values are U,7.

SUSPEND - Not valid for use.

SWAP - SWAP controls the swapping of the TSS address space by the MVS operating system. The recommended operand value is NO.

SYNCH - Not valid for use.

SYSOUT - Not valid for use.

TAPE - The TAPE option specifies the type of tape protection (if any) that is in effect at your ADP activity. The required operand is the default value of OFF.

TIMER - TIMER controls the interval at which data is written to TSS buffers. This includes writing IMS and CICS transaction events to SMF. The recommended value for this operand is 30.

TSS - Not valid for use.

VERSION - Not valid for use.

VTHRESH - The VTHRESH option: 1) selects an access violation threshold for on-line user, batch jobs and started tasks, and 2) selects the action that TSS will take when the threshold is reached. The required operand values are 4,SUS.

WHOOWNS - Not valid for use.

APPENDIX D

COMPUTER FRAUD AND ABUSE ACT OF 1986

The below is a paraphrased version of the Computer Fraud and Abuse Act of 1986 (P.L. 99-474) as it applies to this technical publication. The sections of the Act not covered below concern classified information and information subject to the Atomic Energy Act of 1954, the Right to Financial Privacy Act of 1978, and the Fair Credit Reporting Act.

UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE.

Public Law 99-474, Chapter XXI, Section 1030, states that "whoever knowingly ...., or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, ... obtains ..., alters, damages, destroys, or discloses information ..., or prevents authorized use of (data or a computer owned by or operated for) the government of the United States ... shall be punished (by) ... a fine under this title or imprisonment for not more than 10 years, or both".

REPORT UNAUTHORIZED USE OR ACCESS TO THE DESIGNATED OFFICE OR INDIVIDUAL RESPONSIBLE FOR COMPUTER SECURITY MATTERS.

APPENDIX E

DATA ACCESS REFERENCES

INTRODUCTION. This appendix provides a list of documents and guidance published by the cognizant Functional Managers that govern the authorization of access and administration of the data associated with their systems.

1. CMC letter 5500, MPI-50 of 1 May 1986, MANPOWER DATA-ACCESS SECURITY POLICY.

2. CMC letter 5510, FDA-54 of 7 May 1987, STANDING OPERATING PROCEDURES (SOP) FOR FISCAL DIVISION CLASS I ACCOUNTING AND BUDGETING AUTOMATED INFORMATION SYSTEM DATA SECURITY.

3. MCO P5500.15, FD-MCFC-DAPS-2 OF 14 July 1988, FINANCIAL AUTOMATED INFORMATION SYSTEM (AIS) SECURITY MANUAL.

4. Request for access to data from CLASS I Marine Corps Logistics Systems will be addressed to DC/S for Installation & Logistics (CMC Code LPS). Washington, DC 20380-0001.

5. Request for access to data from Marine Corps Aviation Systems will be addressed to DC/S for Aviation (CMC Code A), Washington, D.C. 20380-0001.

COMMENTS/REVISIONS

Technical publications under the Information Resources Management (IRM) Standards and Guidelines Program (MCO 5271.1) are reviewed annually. Your comments and/or recommendations are strongly encouraged.

IRM Tech Pub Name: _____

IRM-____-___ (Number) Date of Tech Pub: _____

COMMENTS/RECOMMENDATIONS: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Name/Rank: _____(optional)

Unit: _____(optional)

Mail To: Commandant of the Marine Corps (Code CCIS)
Headquarters, United States Marine Corps
Washington, D.C. 20380-0001