DNOS

Security Manager's Guide

Part No. 2308954-9701 **
15 November 1983

TEXAS INSTRUMENTS

MANUAL REVISION HISTORY

DNOS Security Manager's Guide (2308954-9701)

Original Issue ..... 15 November 1983

The total number of pages in this publication is 62.

The computers offered in this agreement, as well as the programs that TI has created to use with them, are tools that can help people better manage the information used in their business; but tools—including TI computers—cannot replace sound judgment nor make the manager's business decision.

Consequently, TI cannot warrant that its systems are suitable for any specific customer application. The manager must rely on personal judgment of what is best for his or her business.

DNOS Software Manuals

This diagram shows the manuals supporting DNOS, arranged according to user type. Refer to the block identified by your user group and all blocks above that set to determine which manuals are most beneficial to your needs.

All DNOS Users:

- DNOS Concepts and Facilities 2270501-9701
- DNOS Operations Guide 2270502-9701
- DNOS System Command Interpreter (SCI) Reference Manual 2270503-9701
- DNOS Text Editor Reference Manual 2270504-9701
- DNOS Messages and Codes Reference Manual 2270506-9701
- DNOS Reference Handbook 2270505-9701
- DNOS Master Index to Operating System Manuals 2270500-9701

High-Level Language Users:

- COBOL Reference Manual 2270518-9701
- DNOS COBOL Programmer's Guide 2270516-9701
- DNOS Performance Package Documentation 2272109-9701
- TI Pascal Reference Manual 2270519-9701
- DNOS TI Pascal Programmer's Guide 2270517-9701
- FORTRAN-78 Reference Manual 2268681-9701
- DNOS FORTRAN-78 Programmer's Guide 2268680-9701
- MATHSTAT-78 Programmer's Reference Manual 2268687-9701
- FORTRAN-78 ISA Extensions Manual 2268696-9701
- TI BASIC Reference Manual 2308769-9701
- RPG II Programmer's Guide 939524-9701

Assembly Language Users:

- 990/99000 Assembly Language Reference Manual 2270509-9701
- DNOS Assembly Language Programmer's Guide 2270508-9701
- DNOS Link Editor Reference Manual 2270522-9701
- DNOS Supervisor Call (SVC) Reference Manual 2270507-9701

Security Managers:

- DNOS Security Manager's Guide 2308954-9701

Productivity Tools Users:

- DNOS Sort/Merge User's Guide 2272060-9701
- DNOS TIFORM Reference Manual 2276573-9701
- DNOS Query-990 User's Guide 2276554-9701
- DNOS Data Base Management System Programmer's Guide 2272058-9701
- DNOS Data Base Administrator User's Guide 2272059-9701
- Data Dictionary User's Guide 2276582-9701
- DNOS TIPE Reference Manual 2308786-9701
- DNOS TIPE Exercise Guide 2308787-9701
- DNOS COBOL Program Generator User's Guide 2234375-9701

Communications Software Users:

- DNOS DNCS/SNA User's Guide 2302663-9701
- DNOS DNCS Operations Guide 2302662-9701
- DNOS DNCS 914A User's Guide 2302664-9701
- DNOS 3270 Interactive Communications Software (ICS) User's Guide 2302670-9701
- DNOS 3780/2780 Emulator User's Guide 2270520-9701
- DNOS DNCS System Generation Reference Manual 2302648-9701
- DNOS DNCS X.25 Remote File Transfer (RFT) User's Guide 2302640-9701
- DNOS Remote Terminal Subsystem (RTS) User's Guide 2302676-9701

Systems Programmers:

- DNOS System Generation Reference Manual 2270511-9701
- DNOS Systems Programmer's Guide 2270510-9701
- DNOS Online Diagnostics and System Log Analysis Tasks User's Guide 2270532-9701
- ROM Loader User's Guide 2270534-9701

Source Code Users:

- DNOS System Design Document 2270512-9701
- DNOS SCI and Utilities Design Document 2270513-9701

DNOS Software Manuals Summary

Concepts and Facilities
Presents an overview of DNOS with topics grouped by operating system functions. All new users (or evaluators) of DNOS should read this manual.

DNOS Operations Guide
Explains fundamental operations for a DNOS system. Includes detailed instructions on how to use each device supported by DNOS.

System Command Interpreter (SCI) Reference Manual
Describes how to use SCI in both interactive and batch jobs. Describes command procedures and gives a detailed presentation of all SCI commands in alphabetical order for easy reference.

Text Editor Reference Manual
Explains how to use the Text Editor on DNOS and describes each of the editing commands.

Messages and Codes Reference Manual
Lists the error messages, informative messages, and error codes reported by DNOS.

DNOS Reference Handbook
Provides a summary of commonly used information for quick reference.

Master Index to Operating System Manuals
Contains a composite index to topics in the DNOS operating system manuals.

Programmer's Guides and Reference Manuals for Languages
Contain information about the languages supported by DNOS. Each programmer's guide covers operating system information relevant to the use of that language on DNOS. Each reference manual covers details of the language itself, including language syntax and programming considerations.

Performance Package Documentation
Describes the enhanced capabilities that the DNOS Performance Package provides on the Model 990/12 Computer and Business System 800.

Link Editor Reference Manual
Describes how to use the Link Editor on DNOS to combine separately generated object modules to form a single linked output.

Supervisor Call (SVC) Reference Manual
Presents detailed information about each DNOS supervisor call and DNOS services.

DNOS System Generation Reference Manual
Explains how to generate a DNOS system for your particular configuration and environment.

User's Guides for Productivity Tools
Describe the features, functions, and use of each productivity tool supported by DNOS.

User's Guides for Communications Software
Describe the features, functions, and use of the communications software available for execution under DNOS.

Systems Programmer's Guide
Discusses the DNOS subsystems and how to modify the system for specific application environments.

Online Diagnostics and System Log Analysis Tasks User's Guide
Explains how to execute the online diagnostic tasks and the system log analysis task and how to interpret the results.

ROM Loader User's Guide
Explains how to load the operating system using the ROM loader and describes the error conditions.

DNOS Design Documents
Contain design information about the DNOS system, SCI, and the utilities.

DNOS Security Manager's Guide
Describes the file access security features available with DNOS.

Preface

This manual describes the DNOS security features that are available to help you protect a system against the following:

- Illegal access to important systems areas by unauthorized users.
- Attempts to destroy or alter data.

DNOS does not have the capability to protect a system against the attempts of systems programmers to gain access to key system areas or secured files. Instead, you would need to take physical security measures against such attempts. Also, you should not leave this manual out for general reading. Since it tells you how to protect your system, it can also tell someone else how to break into your system.

This manual contains the following sections:

Section

1 Introduction — Describes the types of security features that are and are not available with DNOS.

2 DNOS File Security Concepts — Describes the concepts necessary to understand security on a DNOS system: access groups, access rights, and careful security management.

3 Planning the Security Environment — Describes what a security manager needs to keep in mind when planning a security environment.

4 Creating the Security Environment — Gives a step-by-step description of what a security manager needs to do to create the security environment.

5 Maintaining the Security Environment — Describes what responsibilities a security manager has in maintaining the security environment.

6 Special Problems — Describes how a security manager can deal with special security problems.

The DNOS software manuals shown on the support manual diagram (frontispiece) contain related information.

Contents

4 — Creating the Security Environment

5 — Maintaining the Security Environment

6 — Special Problems

Index

Illustrations

Tables

1

General Information

1.1 INTRODUCTION

Remote computer access and distributed processing make database security and file security more important than ever. An operating system cannot possibly ensure complete security, but DNOS provides various security features that a security manager can use to build a safeguarded system. Texas Instruments does not set up a DNOS security system; rather, you select the security features most appropriate for your system environment.

Security on a DNOS system is an option you can choose during system generation. A DNOS system with the security option is called a secure system. However, this fact does not mean you have a useful security system. Selecting the security option only makes a selection of certain security features possible on the system. You must choose which ones to use.

You are responsible for the following:

- Planning the security environment
- Creating the security environment
- Maintaining the security environment
- Managing special problems

Use this guide to learn what system tools are available and how you can use them to secure your system.

This section describes the types of security features that are and are not available with DNOS.

1.2 SECURITY FEATURES AVAILABLE WITH DNOS

In general, security of a system is realized by meeting the following objectives:

- Requiring proper identification when users enter the system and recording attempts at illegal access
- Preventing illegal access to user files and system resources
- Preventing unauthorized access to important applications

The following paragraphs describe the security features DNOS has to meet these objectives.

1.2.1 Requiring Proper Identification

Assigning user IDs and passcodes provides system access security. When terminals are defined to require logon, only users with valid user IDs and passcodes can log on the system. DNOS writes a message to the system log after three invalid attempts to log on a given terminal.

1.2.2 Preventing Illegal Access to User Files and System Resources

You can safeguard files by taking the following measures:

- Select file security support during system generation.
- Set up basic security groups and user IDs before allowing the users to log on. These groups are called access groups and are described in the next section. Access to files can be limited to specific access groups.
- Secure disk volumes that are to be used only on systems that support file security.
- Encrypt data in particularly sensitive files.

Lists of critical system resources are provided in this manual to guide you in securing the system files in which they are contained.

You can make disk volumes that are installable only on systems with file security. However, volumes developed on DX10 systems or DNOS systems without security can be used on any DNOS system.

1.2.3 Preventing Unauthorized Access to Important Applications

You can help safeguard the operating system by restricting certain command procedures to particular groups of users. You can also limit users by preventing them from issuing SCI primitives.

1.3 SECURITY FEATURES NOT AVAILABLE ON DNOS

The following security features are not available with DNOS:

- Device security
- Logging file security violations
- Record level security in a file (this feature is available, however, on DBMS 990, the database management system for the 990 computer)
- Security against modification of data or task segments while they are in memory
- Automatic clearing of memory or disk when space is released
- Directory level security

DNOS does not automatically prohibit access to all files under a directory. To secure a directory, you must secure each file within it.

2

DNOS File Security Concepts

2.1 INTRODUCTION

In a DNOS system using file security, a user can perform an operation on a file only if the following two conditions are met:

- The user is a member of an access group that has access rights to the file.
- The operation is allowed by the access rights that the access group has to the file.

You should refer to the *DNOS System Command Interpreter (SCI) Reference Manual* for explanations concerning any commands with which you are not familiar. Most of the SCI commands that are related to security require you to enter your log-on passcode as an additional precaution. Therefore, when you have a file security environment, you should make sure that user IDs without passcodes have only limited capabilities on the system.

2.2 ACCESS GROUPS

An access group is composed of a set of user IDs. The users of these IDs usually have a common work assignment or a common need for system resources.

The name of an access group must be a string of one to eight alphanumeric characters, with the first character alphabetic. A user's rights to particular files on the system are assigned by access group name. Each secured file on the system can have access rights defined for up to nine access groups. You can define a different set of rights for each group.

There are two types of access groups: predefined and user-defined. PUBLIC and SYSMGR are the only two predefined access groups. Belonging to PUBLIC is the lowest form of membership on the system; belonging to SYSMGR is the highest.

Everyone on the system is automatically an access group member of PUBLIC. A user who belongs only to the PUBLIC access group has rights only to unsecured files and files that have specific rights defined for the PUBLIC access group.

Usually, only the security manager or a small, trusted group belongs to the SYSMGR access group. The SYSMGR group has access rights to every file and implied leadership of every access group.

All other access groups on the system are user-defined and are created for a specific purpose. The creator of an access group automatically becomes the initial access group leader. The leader designates which users on the system are members of his access group. A user can be a leader of one or more access groups and also a member in others.

After creating a file, a user can specify which access groups are allowed access to it and the types of access these groups can have.

The roles one can play in access groups are briefly described in the following paragraphs.

2.2.1 SYSMGR Access Group Member

As the security manager, you are normally either the only member of the SYSMGR access group or the leader of a small, trusted group. The system automatically creates the SYSMGR access group. The system creates it with a user ID named SYSMGR as the leader of the access group. If you want anyone else to be a member of the SYSMGR access group, you must assign a user ID to that person and explicitly include that user ID as a member of the SYSMGR access group.

The SYSMGR access group should be used only in unusual situations when the file security system needs to be circumvented. Anyone who logs on with a user ID that is a member of the SYSMGR access group is given full access rights to every file on the system and the ability to assume leadership of any access group except SYSMGR.

Since membership in the SYSMGR access group gives so much capability, user IDs in this group should not be used for routine work assignments. The SYSMGR access group should be used only when it is necessary to bypass the file security system. Such times include the following:

- When applying patches supplied by Texas Instruments.
- When a person who is an access group leader leaves (vacation, illness, and so on) and does not specify a new access group leader beforehand.
- When someone needs to access a particular file and no one who has control of the file can be found.

The user IDs in the SYSMGR access group are not allowed to be members of other access groups. If a member of SYSMGR tries to create an access group or to modify an existing access group to make his user ID a member of the group, the system returns an error. Therefore, you will want to assign each person who has a user ID that is a member of the SYSMGR access group another user ID for routine work operations.

As the security manager, you will want a third user ID to create and maintain the security environment. This user ID will be the leader of an access group (known as the security manager maintenance access group) that will have exclusive access to various system files. (Tables in Section 4 of this manual indicate which system files are to be secured to yourself.) Limiting certain system files to yourself will allow you to control who can log on to certain terminals, who can add or delete user IDs, and who can access certain system resources. Since you will give this third user ID full access rights to sensitive files, do not use it for routine work assignments; use it only when necessary.

2.2.2 Access Group Leader

A user on the system becomes an access group leader either by creating an access group or by having the leader of an access group give up his leadership and designate him as the new leader.

Each access group has only one leader (however, any member of the SYSMGR access group can perform any function the leader can). The access group leader controls membership in the group by his right to add, delete, or list members. To create an access group, a user must have access to the Create Access Group (CAG) command procedure. You can limit the proliferation of access groups by restricting the CAG command procedure to certain users.

2.2.3 Access Group Member

An access group member is a person whose user ID belongs to the set of user IDs for a specific access group. Only the access group leader (and members of the SYSMGR access group) can add, delete, or list access group members. An access group member shares the access rights of his group to files on the system. Every user is a member of at least one access group since all users of the system belong to PUBLIC.

2.2.4 Creation Access Group

Every user on the system has exactly one creation access group. A user can select one of the access groups to which he belongs as his creation access group. A user makes this selection by executing the Set Creation Access Group (SCAG) command. If a user never specifies a particular group, his creation access group is PUBLIC by default.

A user's creation access group initially inherits all access rights (control, read, write, execute, and delete) to any files that a user creates under his user ID. This includes files created explicitly with the Create File (CF) command, as well as files created by tasks running in the user's job.

As long as the creation access group retains control access, only users who belong to the group (or members of SYSMGR) can give any access rights to a file to other access groups (by executing the Modify Security Access Rights (MSAR) command). Giving read, write, execute, or delete access rights to another group does not take away these rights from a user's own group. However, since only one access group can have control access to a file, giving control access to another access group means taking it it away from the user's group. Therefore, a user should be very careful before assigning control access for a file to another access group.

For example, a user selects an access group called LAWYERS as his creation access group. He logs off and logs on again (the system recognizes the selection only in this manner). Then, he creates a file called ACCOUNTS. The LAWYERS access group now has control, read, write, execute, and delete access to ACCOUNTS. Later, he decides that a related access group, called PARALGLS should have read access and write access to the file. He would then use the MSAR command to assign them these two rights. Later, unknown to him, a junior member of LAWYERS uses the MSAR command to assign control access to the PARALGLS access group. The next time he tries to assign access rights to ACCOUNTS with the MSAR command, he will receive an error, since his access group, LAWYERS, no longer has control access to the file. After locating and taking appropriate revenge on the junior member of LAWYERS who gave the file away, he would have to talk one of the members of PARALGLS (or a member of SYSMGR) into using the MSAR command to return control access to LAWYERS.

2.2.5 Modifications to Access Groups and Access Rights

The system determines what access groups a user belongs to when a job is created with his user ID. Therefore, for the system to recognize any selection or modification that involves access groups, the user affected by such a change must log off and then log back on again for the change to take place. Changes to membership in an access group or to the selection of a current creation access group do not affect running jobs.

Modifications to the access rights of a file take effect immediately. However, the system determines a user's access rights to a file when he tries to assign a LUNO to the file. Therefore, if a LUNO is already assigned to a file by a job, the job will execute regardless of any changes to the file's security.

For example, you are running a job that uses a file to which your access group has all access rights. If someone uses the MSAR command to take away all the access rights to the file, the job you are running may or may not be affected. If a LUNO is already assigned to the file, the modification will not affect the running job. However, if the LUNO has not been assigned, an error occurs when the task (under which the job is running) tries to access the file for which you no longer have access rights.

2.3 ACCESS RIGHTS

There are five possible types of access rights to a file:

- Control access
- Read access
- Write access
- Execute access
- Delete access

The access rights that an access group possesses define what ways its members can use a particular file.

Only one access group can have control access to a file. However, a member of an access group that has control access to a particular file can give any access group any combination of the last four rights to the file.

You can use the MSAR command to assign or alter access rights to a file. When securing a file, you should carefully consider security requirements before deciding which groups should have access rights to the file. You should consider whether or not certain access rights can be withheld without affecting the normal work of the users. The following paragraphs describe each of the access rights.

2.3.1 Control Access

Control access is the right to change the access groups associated with a file or to change the access rights of any access group. Only one access group can have control access to a particular file. You must be a member of an access group that has control access to a file in order to execute the MSAR command on that file.

2.3.2 Read Access

Read access is the right to read the contents of a file. This right also enables you to execute a file if it is an SCI batch stream or command procedure. If the file is a program file, read access allows you to designate the file when issuing the Map Program File (MPF) and Show Program Image (SPI) commands. With read access to a file, you can copy the contents of the file into any file for which you have write access.

2.3.3 Write Access

Write access is the ability to write data into a file. It allows you to modify old data and write new data. In addition, write access to a program file enables you to install or delete tasks, segments, procedures, and overlays. If the file is a key indexed file, this right allows you to insert or delete records from the file.

2.3.4 Execute Access

Execute access applies only to program files. This right allows you to execute tasks, segments, procedures, and overlays within a program file. As a security measure, you can protect your powerful or sensitive tasks by placing them in a protected program file. However, do not move tasks supplied by Texas Instruments, as this step would affect the ability of the system to accept Texas Instruments patches.

2.3.5 Delete Access

Delete access is the right to delete (or replace) a file. In order to text edit a file, you must have both write and delete access.

2.4 EXAMPLE OF A SECURED SYSTEM

Figure 2-1 shows the relationship between access groups and access rights to particular files. Imagine a system that currently has only two user-defined access groups (ADMIN and FINANCE) and two secured files (ACCOUNTS and BILLING). PRES is the access group leader for ADMIN. He has designated ADMIN as his creation access group.

In this system, PRES can read both of the secured files because read access to these files has been defined for the ADMIN access group. He can also write to the BILLING file. ANALYST can write to ACCOUNTS because write access to the file has been defined for the FINANCE access group. However, if he tries to write to the BILLING file, he will receive an error because write access has not been defined for his access group.

ACCESS GROUP	IDS OF MEMBERS
ADMIN	PRES, VP
FINANCE	CMPTRLR, ANALYST, CLERK1, CLERK2

SECURED FILE	ACCESS GROUP	ACCESS RIGHTS
ACCOUNTS	ADMIN	READ, DELETE, CONTROL
	FINANCE	READ, WRITE
BILLING	ADMIN	READ, WRITE, DELETE, CONTROL
	FINANCE	READ

2284929

Figure 2-1. Access Groups and Secured Files

Consider that PRES needs to modify the accounts that his company has. To do so, he must establish write access to the ACCOUNTS file. Because he belongs to the ADMIN access group (which has control access to that file), he may issue the MSAR command to give write access to ADMIN.

Consider that ANALYST was convinced he could help ADMIN modify the BILLING file. He has two options. First, he could ask PRES (the access group leader) to include his user ID in the ADMIN access group. Second, he could ask anyone in the ADMIN access group to modify the security of the file in order to give write access to his access group, FINANCE.

Consider that PRES wants to create a stock strategy file which only the PRES, VP, and CMPTRLR can access. He can create an access group called LEADERS by executing the CAG command. PRES automatically becomes access group leader of LEADERS because he executed the command. If he wants to add members, delete members, or designate a new leader he must execute the MAG command. Then, he can use the Create File (CF) command to create a file named STRATEGY. The ADMIN group now has all access rights to the file (because PRES has selected ADMIN as his creation access group). He can then execute the MSAR command to define what access rights he wants the LEADERS access group to have.

After these operations, the system would have one additional access group and one additional secured file, which might appear in Figure 2-2.

ACCESS GROUP	IDS OF MEMBERS
LEADERS	PRES, VP, CMPTRLR

SECURED FILE	ACCESS GROUP	ACCESS RIGHTS
STRATEGY	ADMIN	READ, WRITE, DELETE, CONTROL
	LEADERS	READ, WRITE

2284930

Figure 2-2. Creating an Access Group

2.5 IMPORTANT POINTS ABOUT ACCESS RIGHTS TO SECURED FILES

Each secured file can have access rights defined for up to nine access groups. The MSAR command assigns access rights and modifies them. You can define a different set of rights for each group.

The rights granted to an access group define the rights of each member. The rights of an individual user are determined by membership in access groups. A user can access a file only if he is part of an access group that has rights to the file.

The rights to a file for a given user are a composite of the rights for all of the access groups to which he belongs. For example, a user is a member of two access groups. The first has read access to a file and the second has write access to the same file. In this case, the user has both read and write access to that file.

Access rights are independent of each other. Any combination of rights can be assigned to a file, even if certain combinations would not appear to make much logical sense.

The system establishes what access groups a user belongs to when a job is created with his user ID.

The system establishes a user's access rights to a file when he assigns a LUNO to the file.

The write-protect, delete-protect mechanisms of the Modify File Protection (MFP) command are independent of file security, except in one way. To use the MFP command on a file, you must have write access and delete access.

Changing the data in a file or the name of a file does not affect the access rights associated with the file. However, if you delete a file and create a new one with the same name, the file is no different from any other that you create under your user ID: your creation access group inherits all access rights to the new file.

Programs that copy files normally read the data from an input file and write the data to an output file. If the copying process is executed with any of the following SCI commands, the security rights of the input file are transferred to the output file.

- BDD — Back Up Directory to Device (followed by the Restore Directory (RD) command)
- CV — Copy Volume
- CVD — Copy Volume to Device
- DCOPY — Disk Copy/Restore

If the copying process is executed with any other command, the security of the input file is not transferred to the output file.

2.6 CAREFUL SECURITY MANAGEMENT

Think carefully about security before system generation. Consider the file structure that you want to use on the system. If you already have current data disks, use the Map Disk (MD) command to discover their present contents. Some of the major questions to ask yourself at this stage are as follows:

- Do you need file security, physical security, or both?
- Who are the users of the system?
- Can you classify your users into distinct groups?
- What kind of user groups do you want?
- Do the user groups consist mostly of programmers? If so, do you have an applications environment or a software development environment?
- What system resources do most users need to have?
- What system resources can be reserved?

You need to answer all of these questions before you implement security. Making major changes to security on a system that already exists can be awkward and expensive. The file structure you design now and the access groups you use will affect the ease of use and security of your system.

The following sections cover these topics:

- Planning the security environment
- Creating the security environment
- Maintaining the security environment

3

Planning the Security Environment

3.1 INTRODUCTION

As security manager, you are responsible for planning the security environment of your system. While planning the security environment, you should carefully consider the requirements for your system. You should also consider whom you want the access group leaders to be. Either you or the access group leaders need to design access groups that are compatible with the file structure of the system and the needs of users.

You also need to give users access to command procedures so that they can perform their work efficiently on a secure system. This section describes the command procedures that are commonly given to general users and access group leaders. This section also helps you understand certain features that are available to programmers.

3.2 DESIGNING THE ACCESS GROUPS

As the security manager, you need to determine the expected use of the system. Make a list of users, their titles, and their departments, so that you may design access groups that use the system's file structures efficiently. The system environment dictates whether your access groups will be static or dynamic.

An applications environment is usually static, and you can design access groups that are fixed. When you identify all the users of the system, you can design the access groups according to responsibilities and needs. You should plan to reserve the Create Access Group (CAG) command for yourself or a small circle of access group leaders.

A software development environment is usually dynamic, and you will have to allow users to develop access groups as their need requires. In this environment, you might allow everyone the right to use the CAG command. If you do allow users to use this command, they must maintain records of the access groups they create and the files those access groups can access.

3.3 THE GENERAL USER

A user who makes use of your system but who has no leadership responsibilities for file security needs few security commands. A general user may belong to one or more access groups or may belong only to PUBLIC. You should allow general users access to only the following file security command procedures:

- Set Creation Access Group (SCAG)
- List Access Groups (LAG)
- List Access Group File Rights (LAGFR)
- List Security Access Rights (LSAR)
- Modify Security Access Rights (MSAR)
- Modify Passcode (MPC)

3.3.1 Set Creation Access Group (SCAG) Command

The SCAG command permits a user to designate one access group (of which he is a member) that will have full access rights to files that he later creates.

3.3.2 List Access Groups (LAG) Command

The LAG command lists (according to user ID), all access groups to which the user belongs. It indicates the access groups of which the user is the leader and the creation access group he has selected. If the user is a member of the SYSMGR access group, the command lists all the access groups in the system.

3.3.3 List Access Group File Rights (LAGFR) Command

The LAGFR command lists all the files under the specified directory to which a particular access group has access rights. The command also lists the access rights of the group for each file listed.

If you specify PUBLIC as the access group, the LAGFR command lists all the files that have been specified for PUBLIC access and files that are unsecured.

3.3.4 List Security Access Rights (LSAR) Command

The LSAR command lists all the access groups that have access rights to a specified file. To use this command, a user must be a member of the access group that has control access to the file.

3.3.5 Modify Security Access Rights (MSAR) Command

The MSAR command can be used to give an access group full or limited access rights to a file. It can also be used to modify the existing access rights of an access group. To use this command, a user must be a member of the access group that has control access to the desired file.

3.3.6 Modify Passcode (MPC) Command

The MPC command replaces a user's current passcode with a new passcode.

3.4 ACCESS GROUP LEADERS

The following commands are used to create access groups and maintain them:

- Create Access Group (CAG)
- Modify Access Group (MAG)
- List Access Group Members (LAGM)
- Delete Access Group (DAG)

The MAG, LAG, and DAG commands can only be used by an access group leader. In a restrictive environment, you might limit access to the CAG command to designated individuals or to yourself. In a less restrictive environment, you might allow anyone access to the command.

3.4.1 Create Access Group (CAG) Command

The CAG command allows a user to create a new access group and designate the user IDs of members who belong to the group. The user issuing the command automatically becomes the access group leader. You cannot execute the CAG command if you are logged on under a user ID that belongs to the SYSMGR access group.

3.4.2 Modify Access Group (MAG) Command

The MAG command allows an access group leader to add or delete user IDs from the access group. The command also allows a leader to give up his own leadership and designate another user ID as the new leader of the group. Members of the SYSMGR access group can add or delete user IDs from any access group.

3.4.3 List Access Group Members (LAGM) Command

The LAGM command allows an access group leader to list the members of the group. Members of the SYSMGR access group can list the members of any access group.

3.4.4 Delete Access Group (DAG) Command

The DAG command allows an access group leader to delete the access group. The DAG command cannot execute unless the user ID for the leader is the only user ID remaining in the group. Because of this fact, the access group leader needs to perform the following operations before executing the command:

1. Determine which files are accessible to the group. You can use the LAGFR command to help in this process.

2. Delete files available to only the access group. If a file is not deleted before the group with which it is associated is deleted, the file is accessible only to the SYSMGR group.

3. Eliminate file access rights for all other files to which the group has access. If the leader does not eliminate access to these files, anyone with access to the CAG command can create a group with the name of the group the leader just deleted and gain access to those files.

4. Use the MAG command to delete all users except the leader from the access group.

Members of the SYSMGR access group can function as the leader to delete any access group.

3.5 PROGRAMMERS

You should be aware of the following facilities that are available to programmers, since they are related to security:

- I/O utility operations that specify a user ID
- Tasks designated as security bypass tasks
- Special Rename File SVC option
- Open routine specifying user ID (S$OPNS)
- No echo option for SCI prompt response
- Read file characteristics security option

3.5.1 I/O Utility Operations That Specify a User ID

In most cases, when a task uses a file, it does so with the access rights of the user ID of the job in which it is running. In other cases, the task may be a special request server that runs in its own job. In the latter case, the task may need to access a file with the access rights of the requesting task. The user ID and passcode of the requesting task are specified as an I/O parameter in the Supervisor Call (SVC) block for I/O utility operations in the request server task. For security bypass tasks, the passcode does not need to be specified. A security bypass task that specifies a user ID in the parameter list does not bypass security checking for the specified I/O operation. Instead, it picks up the access rights associated with the specified user ID. To set up an SVC block that specifies a user ID, refer to the *DNOS Supervisor Call (SVC) Reference Manual*.

The following I/O utility operations may specify a user ID as an SVC block parameter:

- Assign LUNO — This operation assigns a LUNO if the specified user has any access rights to the file. All subsequent I/O operations that use the LUNO are verified against the specified user's access rights.
- Create File — This operation creates a file with full access rights given to the creation access group of the specified user.
- Delete File — This operation deletes a file if the specified user ID has delete access to the file.

- Unprotect File — This operation removes write and delete protection from a file if the specified user ID has write and delete access to the file.

- Write-Protect File — This operation write protects a file if the specified user ID has write and delete access to the file.

- Delete-Protect File — This operation delete protects a file if the specified user ID has write and delete access to the file.

3.5.2 Security Bypass

Security bypass gives access rights to a program without giving it to the user. The Modify Task Security Attribute (MTSA) command assigns security bypass to a task in a program file; it can also remove this privilege.

A task that is installed with the security bypass attribute is granted access to any file on the system (except when the task uses an I/O utility operation specifying user ID). For this reason, you should secure the MTSA command to yourself, so no one but you can assign the security bypass attribute to a task. It is your responsibility to guarantee the integrity of the task, as the task itself must enforce security. You or a trusted programmer should look over the logic of the task to ensure that no unnecessary files are accessed. Once you have approved the task, you should perform the following steps:

1. Assign the security bypass attribute to the task with the MTSA command.

2. Use the MSAR command to give the control, delete, and write access rights for the program file to your security manager maintenance group. With read and execute access, the user can use the program file for the needed purpose but he does not have the ability to modify it.

3. Write protect the program file for the task, so the file cannot be modified.

A security bypass task that uses one of the I/O utility operations that specify user ID is affected as follows:

- The task inherits the access rights of the user ID specified rather than the full access rights normally given to a security bypass task.

- The task does not need to specify the user passcode in the SVC parameter list.

To set up an SVC block for I/O utility operations that specify user ID, refer to the *DNOS Supervisor Call (SVC) Reference Manual*. Having a security bypass task use one of these operations is useful in cases where you want to give a task unlimited access to files during execution but you want normal file access security for input and output files.

For example, you are willing to give the security bypass attribute to a user's task but you want to guarantee that he can only place the output from the task into files for which the user has access rights. You can limit the user in this way by having the task use an Assign LUNO SVC that specifies his user ID when the task attempts to place the output in a specified file. At this point, the task loses its security bypass attribute. Therefore, before assigning the LUNO, the system checks whether the user has the proper access rights to the output file.

3.5.3 Special Rename File SVC Option

With the normal execution of the Rename File SVC, the new file assumes the security of the old file. For example, if you are modifying a file called LIST1 to be called LIST2, the LIST2 file assumes the security that belonged to LIST1.

However, the special Rename File option allows you to keep the security of the destination file (if it exists) rather than that of the source file. Refer to the *DNOS Supervisor Call (SVC) Reference Manual* for details about this option.

You can use the option under the following three conditions:

- The destination file already exists.
- The replace option is specified.
- You have delete access to both the source file and the destination file.

For example, a source file called ACCOUNT1 and a destination file called ACCOUNT2 already exist on the system. If a programmer elects to use the special option, the Rename File SVC works as follows:

1. .ACCOUNT1 is renamed .ACCOUNT2.
2. The new .ACCOUNT2 file assumes the security of the old .ACCOUNT2 file.
3. The old .ACCOUNT2 file is deleted.

3.5.4 Open Routine Specifying User ID (S$OPNS)

The S$OPNS routine performs the following functions:

- Executes an Assign LUNO SVC, specifying a user ID.
- Opens a user-specified file, a user-specified device, or the Terminal Local File (TLF) for write access. To perform the S$OPNS routine, refer to the *DNOS Systems Programmer's Guide*.

A programmer should use this routine instead of the standard S$OPEN routine when the following two conditions are true:

- The calling task is a security bypass task.
- A standard security check on the listing file is desired. Therefore, a user who executes the task cannot place the output in a file for which he does not have access.

3.5.5 No-Echo Option for SCI Prompt Response

When writing SCI prompts, a programmer can use the no-echo option to indicate that data entered into a field is not to be displayed. Refer to the *DNOS System Programmer's Guide* for details.

3.5.6 Read File Characteristics Option

The Read File Characteristics operation of the I/O SVC has an option that allows the issuer of the SVC to determine what rights he has to a file. If the option is specified, the SVC returns a word of data in the specified buffer. The data indicates what access rights the issuer of the SVC has to the file.

The issuer of the SVC can also determine what access rights another user has to a file. If the user has access rights, and an Assign LUNO Specifying User ID operation was previously performed, then the LUNO assigned can be used with this SVC.

Refer to the *DNOS Supervisor Call (SVC) Reference Manual* for details about this option.

4

Creating the Security Environment

4.1 INTRODUCTION

This section gives a step-by-step description of what you need to create the file security environment. The steps are as follows:

- Selecting security as a system generation option
- Logging on
- Setting up additional IDs
- Securing command procedures
- Assigning user IDs to access groups
- Creating access groups
- Securing sensitive files
- Securing system resources

In addition, this section suggests some optional measures:

- Locking up user command procedure directories
- Using the M$00 command procedure
- Assigning a terminal to a specified set of users

4.2 SELECTING SECURITY AS A SYSTEM GENERATION OPTION

One of the first questions DNOS asks you during system generation is whether you want to use security on the system. To select security, answer YES to the SECURITY? prompt.

If you elect to have security, the following events occur:

- All security code is linked into the operating system.
- SVCs to encrypt and decrypt data are included in the system.
- The operating system (DNOS versions 1.2 and later) creates a user ID (SYSMGR) during the first Initial Program Load (IPL). It also creates an access group with the name SYSMGR.

4.3 LOGGING ON

You must use SYSMGR as your user ID the first time you log on the DNOS system. DNOS defines this user ID. Refer to the *DNOS Operations Guide* for information on how to log on. If you wish, you may later change your ID from SYSMGR to another name. Next, you should assign a passcode to your SYSMGR ID with the Modify Passcode (MPC) command. As a security precaution, you should use the MPC command to change your passcode from time to time. Since there is no way to determine anyone's current passcode, you must keep track of your own passcode.

4.4 SETTING UP ADDITIONAL IDS

Since the SYSMGR access group should be limited to special operations, you should not often need to log on under your user ID in that group. Therefore, you usually need to work outside the SYSMGR access group. Set up two additional access groups (with a user ID for each group) on the system for yourself:

- A security manager maintenance access group and user ID
- A routine work assignment access group and user ID

You can set up a security manager maintenance access group by the following steps:

1. Use the Assign User ID (AUI) command to assign a user ID to yourself. The following is an example of this step:

```
[AUI]

ASSIGN USER ID
          USER DESCRIPTION: BARDAIN
               NEW USER ID: KYLE
              NEW PASSCODE: EIRANNAC
USER PRIVILEGE CODE (0..7): 7
```

2. Log off and then log back on with the user ID you just assigned yourself.

3. Use the Create Access Group (CAG) command to set up the security manager maintenance access group.

```
[CAG]

CREATE ACCESS GROUP

     ACCESS GROUP NAME: SECMGR
        ADD USER ID(S):
```

Remember that the issuer of the CAG command becomes the access group leader. Therefore, you do not need to specify your ID in the ADD USER ID(S) prompt. In this example, KYLE becomes the leader of an access group called SECMGR, of which KYLE is the only member.

4.5 SECURING COMMAND PROCEDURES

Using the Modify Security Access Rights (MSAR) command, you should secure the following command procedures to your security manager maintenance access group:

- Assign User ID (AUI) Command — The AUI command assigns user IDs, passcodes, user privilege codes, and user descriptions.
- Delete User ID (DUI) Command — The DUI command deletes a user's identification information and prevents the user from accessing the system.
- List User IDs (LUI) Command — The LUI command displays a list of the user IDs that are currently defined. The information displayed includes each user ID, the user description for the ID, and the SCI command privilege level for the ID.
- Modify User ID (MUI) Command — The MUI command can modify the passcode or the privilege code associated with a user ID. It cannot modify the ID itself.
- Modify Volume Security (MVS) Command — The MVS command specifies whether a volume is secure or nonsecure. (A secure volume cannot be installed on a DX10 system or a nonsecure DNOS system.)
- Modify Task Security Attribute (MTSA) Command — For a task in a program file, the MTSA command gives or removes the security bypass attribute. A task that has the security bypass attribute can access any file in the system without a security check.

For full details about the commands, refer to the *DNOS System Command Interpreter (SCI) Reference Manual.*

You can deduce the file name for any command procedure on the system according to the following scheme:

.S$CMDS.<SCI command name>

For example, .S$CMDS.AUI is the file name for the Assign User ID command procedure.

The following is an example of securing the LUI command procedure to a security manager maintenance group called SECMGR.

```
[MSAR]

MODIFY SECURITY ACCESS RIGHTS

                PASSCODE:
              FILE NAME: .S$CMDS.LUI
      ACCESS GROUP NAME: SECMGR
            READ ACCESS: YES
           WRITE ACCESS: NO
          DELETE ACCESS: NO
         EXECUTE ACCESS: NO
         CONTROL ACCESS: YES
```

When securing command procedures, perform the following:

- Select YES for the READ ACCESS prompt, since you need to have read access in order to execute an SCI procedure.
- Select NO for the WRITE ACCESS and DELETE ACCESS prompts, since you do not need to have write or delete access to command procedures under your security manager access group. (Selecting NO for these prompts protects you from accidentally deleting or altering command procedures.)
- Select NO for the EXECUTE ACCESS, since command procedure files are not program files.
- Select YES for the CONTROL ACCESS prompt, since every secured file must have one access group that has control access to it.

4.6 ASSIGNING USER IDs

Use the AUI command to assign IDs to all users of the system. User IDs can be up to eight characters long. The first character must be a letter; the rest can be either letters or numbers.

4.7 CREATING ACCESS GROUPS

Use the CAG command to create any access groups you want to include at this stage. From your list of users and user IDs established in the previous step, determine which users should be in the same access groups. Remember that you automatically become the access group leader of any access group you create with the CAG command. If you wish to designate another individual as leader, you must assign leadership to them with the MAG command.

4.8 SECURING SENSITIVE FILES

Use the MSAR command to secure any sensitive files already on your system. Limit access to the access groups that need these files.

4.9 SECURING SYSTEM RESOURCES

A good security system limits access to system resources in an intelligent way. Considering the best tradeoff between security and flexibility in your system environment, you should carefully select the system resources you want to secure. If you do not secure system files to specific access groups, all access rights to those files belong to the PUBLIC access group by default.

The following are common resources you should consider:

- System directories (Table 4-1)
- System files (Table 4-2)
- Command procedures under the .S$CMDS system directory (Table 4-3 through Table 4-8)

You should make all system files necessary for your maintenance duties accessible to your security manager maintenance access group. You should make system files available to other access groups on the basis of need. As an aid, Tables 4-3 through 4-8 outline the resources (and the access rights) that are normally appropriate for different types of users on the system.

To secure a system file, use the following procedure:

1. Use the MSAR command to give control access to the security manager maintenance group.
2. Use the MSAR command again to assign the rights that you want to give to the appropriate access groups.

The following is an example of giving control access of a file (.S$LANG) to a security manager maintenance access group (called SECMGR) and execute access to an access group made up of applications programmers (called APLPRG).

```
[MSAR]

MODIFY SECURITY ACCESS RIGHTS

                  PASSCODE:
                 FILE NAME: .S$LANG
          ACCESS GROUP NAME: SECMGR
                READ ACCESS: NO
               WRITE ACCESS: NO
              DELETE ACCESS: NO
             EXECUTE ACCESS: NO
             CONTROL ACCESS: YES

[MSAR]

MODIFY SECURITY ACCESS RIGHTS

                  PASSCODE:
                 FILE NAME: .S$LANG
          ACCESS GROUP NAME: APLPRG
                READ ACCESS: NO
               WRITE ACCESS: NO
              DELETE ACCESS: NO
             EXECUTE ACCESS: YES
             CONTROL ACCESS: NO
```

To interpret Tables 4-3 through 4-8, use the following key:

Rights	Meaning
C	Control Access — The right to change the access groups associated with a file or change the access rights of any access group.
D	Delete Access — The right to delete or replace a file.
E	Execute Access — The right to execute tasks, segments, procedures and overlays within a program file.
R	Read Access — The right to read a file or execute a file if it is an SCI batch stream or command procedure.
W	Write Access — The right to write data into a file.
N	No Access to Users — This special condition limits all access rights to the SYSMGR access group. To set up this condition, use the MSAR command to assign control access to your security manager maintenance access group; assign no other rights.

Groups	Meaning
APLPRG	Applications Programmers
SECMGR	Security Manager Maintenance Access Group
PUBLIC	PUBLIC Access Group
SYSPRG	Systems Programmers
SYSMGR	SYSMGR Access Group

4.9.1 System Directories

Table 4-1 outlines the system directories (and the access rights) that are normally appropriate for different types of users on the system.

Since you cannot secure a directory, you must secure files one by one. Files under the .S$CMDS directory are special and are discussed later in the section.

Table 4-1. System Directories to Secure

Directory	Description	Rights	Groups
.S$EXPMSG	Files containing expanded error and status messages	R	PUBLIC
.S$MSG	Files containing basic error and status messages	R	PUBLIC
.S$OSLINK	Linkable parts for system generation	R	SYSPRG
.S$ROLLD	System roll file	N	SECMGR
.S$SDTQUE	Files of spooler data, one for each generated system	R	PUBLIC
.SSGU	Files created by system generation	R D	SYSPRG SYSPRG
.S$SYSLIB	Overlay management for automatic overlay loading	R R	APLPRG SYSPRG
.S$SYSTEM	Files containing systems programmers command procedures (excluding software configuration history file (.S$HISTORY), which should have read access allowed for the PUBLIC access group)	R	SYSPRG
.SCI990	Linkable object for the SCI interface (S$) routines	R R	APLPRG SYSPRG

4.9.2 System Files

Table 4-2 outlines the system files (and the access rights) that are normally appropriate for different types of users on the system.

Table 4-2. System Files to Secure

Files	Description	Rights	Groups
.S$ACT1	Accounting log file	R	PUBLIC
.S$ACT2	Accounting log file	R	PUBLIC
.S$CDT	Command definition table	R W	PUBLIC SYSPRG
.S$CLF	Capabilities list file used by SCI commands that affect user IDs (AUI, DUI, LUI, and so on.)	R W	SECMGR SECMGR
.S$CRASH	File to which a system crash can be written	R	SYSPRG
.S$DIAG	File used by online diagnostics when checking the state of the disk	R	PUBLIC
.S$IPL	System loader	N	SECMGR
.S$ISBTCH	Initial batch stream executed during the initialization of the system after an initial program load (IPL)	R W	PUBLIC SYSPRG
.S$LANG	Languages program file	E E	APLPRG SYSPRG
.S$LOG1	System log file	R	PUBLIC
.S$LOG2	System log file	R	PUBLIC
.S$MVI	File used by the Modify Volume Information (MVI) processor to record changes on the disk	R W	SYSPRG SYSPRG
.S$PWCS	Performance microcode	N	SECMGR
.S$SCA	File of information about users that is used by the log-on task and SCI. This file is written to by the Modify Terminal Status (MTS) command	W R	SYSPRG PUBLIC
.S$SECURE	File security program file	E	PUBLIC

Table 4-2. System Files to Secure (Continued)

Files	Description	Rights	Groups
.S$SHARED	Shared program file, used for sharable procedures and special tasks provided by the system	R E	PUBLIC PUBLIC
.S$SHIP	Kernel program file for the system shipped to users	W	SYSPRG
.S$UTIL	System utilities program file	E	PUBLIC
<system name>	Kernel program file created for your system	W	SYSPRG

4.9.3 Command Procedures Under the .S$CMDS Directory

You should consider securing command procedures to only those access groups on your system that need them for their routine assignments. For example, if you have both applications programmers and systems programmers on your system, you can prevent applications programmers from performing unauthorized systems operations by denying them access to command procedures that are appropriate only for systems programmers.

You must decide which users on your system need which command procedures. However, as an aid, the following tables list the command procedures that are usually appropriate for each of the following groups:

- System Operators (Table 4-3)
- Applications Programmers (Table 4-4)
- Systems Programmers (Table 4-5)
- Access Group Leaders (Table 4-6)
- Security Manager Maintenance Access Group (Table 4-7 and Table 4-8)

The command procedures are divided according to their function, not on the basis of their susceptibility to security breaks. Those procedures in the table that are most likely to cause security problems are marked with an asterisk (*).

4.9.3.1 Command Procedures for the PUBLIC access group. To allow general users access to command procedures, simply do not secure the ones you want to give them, since all resources that are not secured belong to the PUBLIC access group.

4.9.3.2 Command Procedures for System Operators. Table 4-3 lists the command procedures that are usually appropriate for system operators. However, if you do not use operators on your systems, these command procedures should then be available to the PUBLIC access group.

Table 4-3. Recommended Command Procedures for System Operators

Command	Full Name of Command
HO	Halt Output at Device
IDT	Initialize Date and Time
KO	Kill Output at Device
KOM	Kill Operator Messages
KOR	Kill Operator Interface Request
LOM	List Operator Messages
LTS	List Terminal Status
LUI*	List User IDs
MDS	Modify Device State
MJP	Modify Job Priority
MO	Modify Output at Device
MSD	Modify Spooler Device
MVI*	Modify Volume Information
QOI	Quit Operator Interface
RO	Resume Output at Device
ROM	Receive Operator Messages
ROR	Respond to Operator Interface Request
XOI	Execute Operator Interface

Note:

* Can cause security problems.

4.9.3.3 Command Procedures for Applications Programmers. Table 4-4 lists the command procedures that are usually appropriate for applications programmers on a system.

Table 4-4. Recommended Command Procedures for Applications Programmers

Command	Full Name of Command
AB*	Assign Breakpoint
ABP*	Assign Breakpoint—Pascal
ASB*	Assign Simulated Breakpoint
CIC	Create IPC Channel
CP	Create Patch
CPI*	Copy Program Image
DB	Delete Breakpoints
DBP	Delete Breakpoints—Pascal
DIC*	Delete IPC Channel
DO*	Delete Overlay
DP*	Delete Procedure Segment
DPB	Delete and Proceed from Breakpoint
DPBP	Delete and Proceed from Breakpoint—Pascal
DPS*	Delete Program Segment
DSB	Delete Simulated Breakpoints
DT*	Delete Task Segment
FB	Find Byte
FW	Find Word
IO*	Install Overlay
IP*	Install Procedure Segment
IPS*	Install Program Segment
IRT*	Install Real-Time Task Segment
IT*	Install Task Segment
LB	List Breakpoints
LBP	List Breakpoints—Pascal
LM	List Memory
LPS	List Pascal Stack
LSB	List Simulated Breakpoints
MIR*	Modify Internal Registers
MM*	Modify Memory
MOE*	Modify Overlay Entry
MPE*	Modify Procedure Segment Entry
MPI*	Modify Program Image
MSE*	Modify Program Segment Entry
MTE*	Modify Task Segment Entry
MWR*	Modify Workspace Registers
PB	Proceed from Breakpoint
PBP	Proceed from Breakpoint—Pascal
QD	Quit Debug Mode
RCRU	Read Contents of Specified CRU Address
RST	Resume Simulated Task

Note:

* Can cause security problems.

Table 4-4. Recommended Command Procedures for Applications Programmers (Continued)

Command	Full Name of Command
SCS	Show Channel Status
SIR	Show Internal Registers
SND	Snapshot Name Definitions
SP*	Show Panel
SPI*	Show Program Image
SPS	Show Pascal Stack
SRF	Show Relative to File
ST*	Simulate Task
SWR*	Show Workspace Registers
WCRU*	Write Value to CRU Address
XD*	Execute in Debug Mode
XLE	Execute Link Editor
XMA	Execute Macro Assembler

Note:

* Can cause security problems.

4.9.3.4 Command Procedures for Systems Programmers. Table 4-5 lists the command procedures that are usually appropriate for systems programmers.

Table 4-5. Recommended Command Procedures for Systems Programmers

Command	Full Name of Command
ALGS	Assemble and Link Generated System
CKD	Check Disk for Consistency
CSF	Create System Files
IGS*	Install Generated System
ISL*	Initialize System Log
LSM*	List System Memory
MAD*	Modify Absolute Disk
MADU*	Modify Allocatable Disk Unit
MCC	Modify Country Code
MCDT	Modify Command Definition Table
MDC	Modify Device Configuration
MLP*	Modify LUNO Protection
MRF*	Modify Relative to File
MSM*	Modify System Memory
MSP	Modify Scheduler/Swap Parameters
MST	Modify System Table Sizes
PGS	Patch Generated System
QSCU	Quit System Configuration Utility Session
RVI	Recover Volume Information
SAD*	Show Absolute Disk
SADU*	Show Allocatable Disk Unit
SCC	Show Country Code
SCDT	Show Command Definition Table
SD	Scan Disk
SGND	Snapshot Global Name Definitions
TGS*	Test Generated System
XANAL*	Execute Crash Analysis Utility
XPD	Execute Performance Display
XSCU*	Execute System Configuration Utility
XSGU*	Execute System Generation Utility

Note:

* Can cause security problems.

4.9.3.5 Command Procedures for Access Group Leaders. Table 4-6 lists the command procedures that are appropriate for access group leaders. As all these commands are marked with an asterisk (*), you can see that they are security sensitive. For further details of these commands, refer to the section in this manual that concerns the planning of the security environment.

Table 4-6. Recommended Command Procedures for Access Group Leaders

Command	Full Name of Command
CAG*	Create Access Group
DAG*	Delete Access Group
LAG*	List Access Groups
LAGM*	List Access Group Members
MAG*	Modify Access Group
SCAG*	Set Creation Access Group

Note:

* Security sensitive.

4.9.3.6 Command Procedures for the Security Manager. Table 4-7 lists the command procedures that are normally appropriate to secure under your security manager maintenance group. As all these commands are marked with an asterisk (*), you can see that they are security sensitive. For further details of these commands, refer to the section in this manual that concerns the planning of the security environment.

Table 4-7. Recommended Command Procedures for the Security Manager

Command	Full Name of Command
AUI*	Assign User ID
DUI*	Delete User ID
IDS*	Initialize Disk Surface
INV*	Initialize New Volume
MTS*	Modify Terminal Status
MTSA*	Modify Task Security Attribute
MUI*	Modify User ID
MVS*	Modify Volume Security

Note:

* Security sensitive.

In addition, you should also consider securing the commands in Table 4-8 to either your security manager maintenance access group or to a special access group of individuals that you trust. As all these commands are marked with an asterisk (*), you can see that they are security sensitive. For a full discussion of the security problems these special volume commands can cause, refer to the section on special problems. The Backup Directory (BD) and Copy Directory (CD) commands are considered safer and may be given to other groups.

Table 4-8. Special Volume Command Procedures

Command	Full Name of Command
BDD*	Backup Directory to Device
CV*	Copy Volume
CVD*	Copy and Verify Disk
DCOPY*	Disk Copy/Restore
RD*	Restore Directory

Note:

* Security sensitive.

4.10 OPTIONAL MEASURES

You may further secure your system by taking the following optional measures.

4.10.1 Locking Up User Command Procedure Directories

You can limit users to the use of command procedure directories designed specifically for their needs. You can then lock up the directories to prevent the command procedures from being modified. You can accomplish these objectives by performing the following steps:

1. Create a limited command procedure directory for each user (for example, .USERCMDS).
2. Write and delete protect each command procedure that you give users.
3. Fill each directory with empty files if the directory is not full. Make sure these empty files are write and delete protected.
4. Prevent users from issuing SCI primitives directly from a terminal or in a batch stream. You accomplish this objective by using the M$00 procedure.

4.10.2 Using the M$00 Command Procedure

You can use the M$00 command procedure to specify certain security limitations on users of a system when they log on. For example, to limit all users except the security manager to a procedure directory called .USERCMDS and to prevent them from using SCI primitives directly from a terminal, you could use the following code:

```
.IF @$$UI,NE,SECMGR
.OPTION PRIMITIVES=NO
.USE .USERCMDS
.ENDIF
```

Also, you can use the M$00 command to place traces into the system log when a certain user (or a group of users) logs on. If you are unfamiliar with using the M$00 procedure, refer to the *DNOS System Command Interpreter (SCI) Reference Manual.* To prevent users from modifying the M$00 procedure, secure the M$00 command procedure to your security manager maintenance access group and give the PUBLIC access group only read access.

4.10.3 Modifying Command Procedures

For special security purposes, you can modify command procedures. For example, you can modify a command procedure to place messages into the system log when a user executes the command. If you are unfamiliar with modifying command procedures, refer to the *DNOS System Programmer's Guide.*

4.10.4 Assigning a Terminal to a Specified Set of Users

You can use the MTS command to define the security for each terminal. In a secure system, you should choose one of the following two options:

- Requiring Users to Log On — To select this option, answer yes to the ASK FOR USER ID? prompt. A user is then required to supply a user ID before the terminal can be operated under SCI.

- Limiting the Terminal to One User ID — To select this option, answer no to the ASK FOR USER ID? prompt. The following set of prompts appear:

```
SUPPLY DEFAULT USER ID
       DEFAULT USER ID: <alphanumeric>
    DEFAULT PASSCODE: <character(s)>
```

By supplying a user ID and passcode, you limit the terminal to SCI operation under one particular user ID. If you also use the M$00 command procedure to limit the terminal user to a specific procedure directory, you can restrict him to using only those commands you wish him to have.

Take special precautions when a terminal on your system is not physically secure. Make sure that any user ID associated with the terminal does not belong to critical access groups.

5

Maintaining the Security Environment

5.1 INTRODUCTION

This section describes the various functions of a security manager when maintaining security on the system. They are as follows:

- Adding a user
- Deleting a user
- Securing and unsecuring volumes
- Monitoring the system log
- Helping users secure their own environments
- Encrypting and decrypting data in files

5.2 ADDING A USER

To add a user to the system, perform the following steps:

1. Use the Assign User ID (AUI) command to assign the user ID.
2. Identify the files and the access rights to those files that the user needs to perform his duties.
3. Determine the access groups to which the user needs to belong.
4. Add the user to these access groups. You can perform this step in one of two ways:
   a. Have the appropriate access group leaders add the user to their groups by executing the Modify Access Group (MAG) command.
   b. Assign the user to the appropriate access groups yourself by executing the MAG command. Here, you must log on with a user ID that is a member of the SYSMGR access group.

5.3 DELETING A USER

To delete a user from the system, perform the following steps:

1. Use the Modify User ID (MUI) command to change the user's passcode. This prevents the user from logging on to the system.

2. Log on with the user's ID.

3. Use the List Access Groups (LAG) command to determine the user's access groups and whether the user is access group leader in any of them.

4. For each access group in which the user is a leader, use the MAG command to give leadership to someone else in the group.

5. For each access group in which the user is the only member, use the following procedure:

   a. Use the List Access Group File Rights (LAGFR) command to see which files are available to the access group.

   b. For each file in which the access group is the only one that has access rights, you have two options. The first option is using the Delete File (DF) command to delete the file. The second option is using the Modify Security Access Rights (MSAR) command to give the access rights to another group and to remove all access rights from the user's access group.

   c. For each file in which the access group shares access rights with other groups, use the Modify Security Access Rights (MSAR) command to remove the group's access rights to the file. Specifying NO to all the access rights prompts deletes a group from the list of groups associated with a file. The following is an example of such an operation:

```
[MSAR]

MODIFY SECURITY ACCESS RIGHTS

                PASSCODE:
                FILENAME: .FILE1
      ACCESS GROUP NAME: USERGRP
            READ ACCESS: NO
           WRITE ACCESS: NO
          DELETE ACCESS: NO
         EXECUTE ACCESS: NO
         CONTROL ACCESS: NO
```

   This operation deletes the user's access group (USERGRP) from the list of access groups associated with .FILE1.

   d. When you have ensured that you have deleted all files associated with the user access group, use the DAG command to delete the group.

6. After you have deleted all the access groups in which the user is the only member, log off and log on again with your security manager maintenance ID.

7. Use the DUI command to delete the user's ID from the system. This step also removes the deleted ID from the remaining access groups to which it belongs (the DUI command does not remove the ID from access groups in which it is the leader, but you have removed it from such groups in a previous step).

5.4 MODIFYING VOLUME SECURITY

Use the Modify Volume Security (MVS) command to secure or unsecure a volume. A secure volume cannot be installed on DX10 systems or on DNOS systems that do not support file security. However, because a secure volume can be installed on any DNOS system that supports security, you should be careful about physical access to removable volumes. System security cannot protect against a user removing a disk. Consider the following possible cases:

- A member of the SYSMGR access group of another system that supports security installs one of your system's removable volumes on his system. Because he is part of the SYSMGR group, he has all access rights to any file that is on the volume.

- One of the users on your system is familiar with most of the access group names. If the user can gain access to another system that supports security, he can install a removable volume on that system. If he has access to the CAG command procedure on that system, he can create access groups that have the same names as access groups on your system that have access rights to files on the removable volume. In this way, a user can gain access rights to files that he could not otherwise access on your system.

To prevent such security problems, you need to take physical security measures.

5.5 ENCRYPTING AND DECRYPTING DATA IN FILES

You have the option of writing a user task that calls upon DNOS to encrypt and decrypt data for any purpose. You can encrypt data of any type.

The DNOS encryption algorithm does not provide a high level of security but does provide a degree of privacy for the data. To write SVCs that encrypt or decrypt data refer to the *DNOS Supervisor Call (SVC) Reference Manual*.

If you require more sophisticated encryption, you must either write your own programs or supply your own SVCs for the purpose.

5.6 MONITORING THE SYSTEM LOG

You should periodically monitor the system log (.S$LOG1 and .S$LOG2) to look for the following violations:

- Illegal logon attempts.
- Entries the spooler places into the system log when a user attempts to print a file for which he does not have read access.
- Entries made by any system log SVC traces that you have included in M$00 or any other commands.

5.7 HELPING USERS SECURE THEIR OWN ENVIRONMENTS

You should instruct users about security maintenance within their own environments. Tell them to do the following:

- Change their passcodes periodically.
- Encrypt data in particularly sensitive files.
- Write and/or delete protect files for which they have control access.

6

Special Problems

6.1 INTRODUCTION

This section describes a system manager's responsibilities with the following special problems:

- Global LUNOs
- Networking
- Copying volumes, directories, and files

6.2 GLOBAL LUNOs

The security manager is responsible for teaching about the danger of using global LUNOs to those persons who use sensitive files and tasks on the system. Global LUNOs pose a security threat for the following reasons:

- Security rights are determined at the time the Assign Global LUNO operation is performed.
- Any job or any task can use a global LUNO.
- If a user creates a task or job that uses a global LUNO, he inherits the access rights of the user who assigned the global LUNO.
- Any user can find out which global LUNOs are assigned to files by using the Show Input/Output Status (SIS) command.

6.3 NETWORKING

If your system is part of a DNOS network, you must carefully consider the security implications of network I/O and network logon. For details about security features available in a DNOS network, refer to the *Distributed Network I/O Object Installation Guide* (part number 2308791-9701).

6.4 COPYING VOLUMES, DIRECTORIES, AND FILES

The command procedures that allow users to copy volumes, directories, and files can pose security problems. These commands fall into two categories:

- Commands that preserve the security of the original but which do not check if the requester of the copy has access rights to the original.
- Commands that check whether the requester has access rights to the original but which do not preserve the security of the original on the copy.

When commands preserve file security, the copy retains the original's list of access groups and access rights. A user has the same access rights to the copy as he had to the original.

When commands check access rights, they copy only the files for which the requester has read access rights. Upon completion of the copy, these commands output a message for each file that is not copied because of insufficient access rights.

Table 6-1 shows which commands preserve file security and which commands check for access rights:

Table 6-1. Copy Commands and Security

Commands	Preserve File Security?	Check Access Rights?
Backup Directory (BD)*	NO	YES
Backup Directory to Device (BDD)*	YES	NO
Copy Directory (CD)	NO	YES
Copy Volume (CV)	YES	NO
Copy Volume to Device (CVD)	YES	NO
Disk Copy/Restore (DCOPY)	YES	NO

Note:

* The Restore Directory Command (RD) must follow these commands.

The CV, CVD, and DCOPY commands copy an entire disk volume of data. The output files, whether they existed previously or not, take on the security of the original files.

The BDD/RD command sequence handles an output file in the following manner:

1. The RD command checks whether the requester has delete access to the output file. If not, it issues a warning message and does not change the output file. Otherwise, it places the output into the file.

2. The output file, whether it existed previously or not, takes on the security of the original file.

The BD/RD command sequence and the CD command handle an output file in the following manner:

- If an output file exists, the CD and RD commands check if the requester has delete access to the file. If not, the commands issue a warning message and do not change the output file. Otherwise, they place the output into the file. The output file retains the security it had before the CD or RD command was performed.

- If an output file does not exist, the CD and RD commands autocreate the file. All access rights to the output file belong to the creation access group of the requester.

You should carefully consider the security implications of copy commands on your system. For example, a person could use the BDD/RD, CV, CVD, and DCOPY commands to copy any file on the system onto a removable volume. Remember, these commands do not check the access rights of the requester. If this person is a user on another secure DNOS system, he could access files on the volume in the following ways:

- If he is a member of the SYSMGR access group, he can access any file on the volume.

- If he has access to the Create Access Group (CAG) command procedure, he can create access groups with the same names as the access groups on the other system. He then inherits the access rights of each of the access groups.

You should consider securing the BDD, CV, CVD, and DCOPY command procedures under one of the following:

- Your security maintenance access group.

- An access group with limited membership (people you trust).

6.5 STATION-LOCAL WORK FILES

Many software products make use of work files that have names with station numbers embedded. For example, a product might use .LIST18 for its listing file at ST18 (a station). Work files of this type are created with the creation access group of the user. If the files are not deleted but the station is used by a second user in a secure environment, the second user may be unable to access the work file (and thereby fail to perform the intended operation) because he does not have the proper access privileges to the file. You or the original user needs to modify the access privileges of the work file or delete it.

Alphabetical Index

Introduction

HOW TO USE INDEX

The index, table of contents, list of illustrations, and list of tables are used in conjunction to obtain the location of the desired subject. Once the subject or topic has been located in the index, use the appropriate paragraph number, figure number, or table number to obtain the corresponding page number from the table of contents, list of illustrations, or list of tables.

INDEX ENTRIES

The following index lists key words and concepts from the subject material of the manual together with the area(s) in the manual that supply major coverage of the listed concept. The numbers along the right side of the listing reference the following manual areas:

- Sections — Reference to Sections of the manual appear as "Sections x" with the symbol x representing any numeric quantity.
- Appendixes — Reference to Appendixes of the manual appear as "Appendix y" with the symbol y representing any capital letter.
- Paragraphs — Reference to paragraphs of the manual appear as a series of alphanumeric or numeric characters punctuated with decimal points. Only the first character of the string may be a letter; all subsequent characters are numbers. The first character refers to the section or appendix of the manual in which the paragraph may be found.
- Tables — References to tables in the manual are represented by the capital letter T followed immediately by another alphanumeric character (representing the section or appendix of the manual containing the table). The second character is followed by a dash (-) and a number.

  Tx-yy

- Figures — References to figures in the manual are represented by the capital letter F followed immediately by another alphanumeric character (representing the section or appendix of the manual containing the figure). The second character is followed by a dash (-) and a number.

  Fx-yy

- Other entries in the Index — References to other entries in the index preceded by the word "See" followed by the referenced entry.

USER'S RESPONSE SHEET

Manual Title: DNOS Security Manager's Guide (2308954-9701)

Manual Date: 15 November 1983 **Date of This Letter:** _____

User's Name: _____ **Telephone:** _____

Company: _____ **Office/Department:** _____

Street Address: _____

City/State/Zip Code: _____

Please list any discrepancy found in this manual by page, paragraph, figure, or table number in the following space. If there are any other suggestions that you wish to make, feel free to include them. Thank you.

Location in Manual	Comment/Suggestion
_____	_____
	_____
	_____
	_____
_____	_____
	_____
	_____
	_____
_____	_____
	_____
	_____
	_____

CUT ALONG LINE

NO POSTAGE NECESSARY IF MAILED IN U.S.A.
FOLD ON TWO LINES (LOCATED ON REVERSE SIDE), TAPE AND MAIL

FOLD

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 7284 DALLAS, TX

POSTAGE WILL BE PAID BY ADDRESSEE

TEXAS INSTRUMENTS INCORPORATED
DIGITAL SYSTEMS GROUP

ATTN: TECHNICAL PUBLICATIONS
P.O. Box 2909 M/S 2146
Austin, Texas 78769

FOLD