SC28-1341-0
File No. S370-34

Program Product

Resource Access Control Facility (RACF) User's Guide

Program Number 5740-XXH

Version 1 Release 6

First Edition (June, 1985)

This edition applies to Version 1, Release 6 of the program product RACF (Program Number 5740-XXH), and to all subsequent versions until otherwise indicated in new editions or Technical Newsletters. Changes are periodically made to the information herein; before using this publication in connection with the operation of IBM systems, consult the latest *IBM System/370 Bibliography*, GC20-0001, for the editions that are applicable and current.

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any references to an IBM program product in this publication is not intended to state or imply that only IBM's program product may be used. Any functionally equivalent program may be used instead.

Publications are not stocked at the address given below; requests for copies of IBM publications should be made to your IBM representative or to the IBM branch office serving your locality.

A form for readers' comments is provided at the back of this publication. If the form has been removed, comments may be addressed to IBM Corporation, Information Development, Department D58, Building 921-2, PO Box 390, Poughkeepsie, N.Y. 12602. IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Who The Audience Is

This book is for the end user who has no knowledge of RACF or who uses RACF infrequently. It is not for you if you wish to understand RACF in technical detail. This book is for you if your concern is the protection of your own data sets or perhaps the data sets belonging to your immediate work group. RACF is capable of much more than what is explained in this book. If you need more technical detail, see one of the publications listed under the title, "Related Publications." This book assumes that you are familiar with a display terminal and how to use TSO. If you are not, we recommend that you become familiar with TSO and TSO commands before using this book.

How To Use This Book

If you are not at all familiar with RACF, start with the background information in "Introduction," which tells you what RACF does, and "How RACF Determines What You Can Do" which defines some terms you will need.

If you know what you want to do, go directly to the task that contains the information you need. The tasks fall into four general sections:

Getting Started tells how to get started using RACF.

Protecting Information Using RACF Commands tells how to protect your information using RACF commands.

Protecting Information Using RACF ISPF Panels tells how to protect your information using RACF ISPF panels.

Miscellaneous describes several miscellaneous tasks related to RACF.

Related Publications

Other books you might find particularly helpful are:

Resource Access Control Facility (RACF): General Information Manual, GC28-0722, presents an overview description of what RACF can do.

Resource Access Control Facility (RACF): Command Language Reference, SC28-0733, contains a complete description of all RACF commands.

Resource Access Control Facility (RACF): Security Administrator's Guide, SC28-1340, contains a complete description of the role of those individuals defined as RACF security administrators. These are individuals who are responsible for implementing data security.

Resource Access Control Facility (RACF): Auditor's Guide, SC28-1342, contains a complete description of the role of those individuals defined as RACF auditors. These are individuals who are responsible for auditing data security.

System Programming Library: Resource Access Control Facility (RACF), SC28-1343. This book is for those individuals who are responsible for installing, maintaining and modifying RACF.

Resource Access Control Facility (RACF): Messages and Codes, SC38-1014, contains a complete description of all RACF messages and the RACF-related system completion codes.

Resource Access Control Facility (RACF): Program Logic Manual, LY28-0730, contains a complete description of the internal logic of RACF.

TSO Command Language Reference, GC28-0646, contains a complete description of all TSO commands.

TSO Terminal User's Guide, GC28-0645, contains a complete description of how to use TSO.

Contents

Figures

INTRODUCTION

No one wants his or her life subject to scrutiny from just anyone. The amount of privacy you need is a very personal matter. In fact, there are areas of your life that are known only to you. In your daily life, you take deliberate steps to maintain your privacy and to prevent unauthorized use of your property. You lock your front door; you don't leave your car keys in the ignition. You expect the professionals, such as the doctors and the lawyers, in your life to keep your records confidential.

You use RACF just as you would lock your door or take your car keys with you. RACF helps you protect your property, your information and your organization's information. Some of your information might not need protection, while other information might be highly sensitive and need protection.

RACF is a tool for protecting information. It helps you get a job done without getting in your way. Because it must meet your needs and your organization's needs and be flexible enough to change as those needs change, it has a complex structure. You, however, need only some basic information about RACF. This chapter presents some basic concepts. "How RACF Determines What You Can Do" describes basic terms you need to use RACF.

If, as you become familiar with RACF, you need to understand RACF in more technical detail, the RACF library contains additional information. The first page of this book lists the RACF books as well as some other books you might find helpful.

What RACF Is

When many individuals must use information, there must be control over who uses the information and how and when they use the information. This control may be hardware; a feature of the machine. For example, a machine might need a key to turn it on or a certain code entered before the machine will run. In a computer system, the control might be software; a program or a set of programs. RACF is a software control mechanism that helps an organization manage access to information.

RACF works much the same way as a large organization works. The president sits at the top, but his or her authority percolates downward to all employees. Figure 1 illustrates a typical organizational structure.

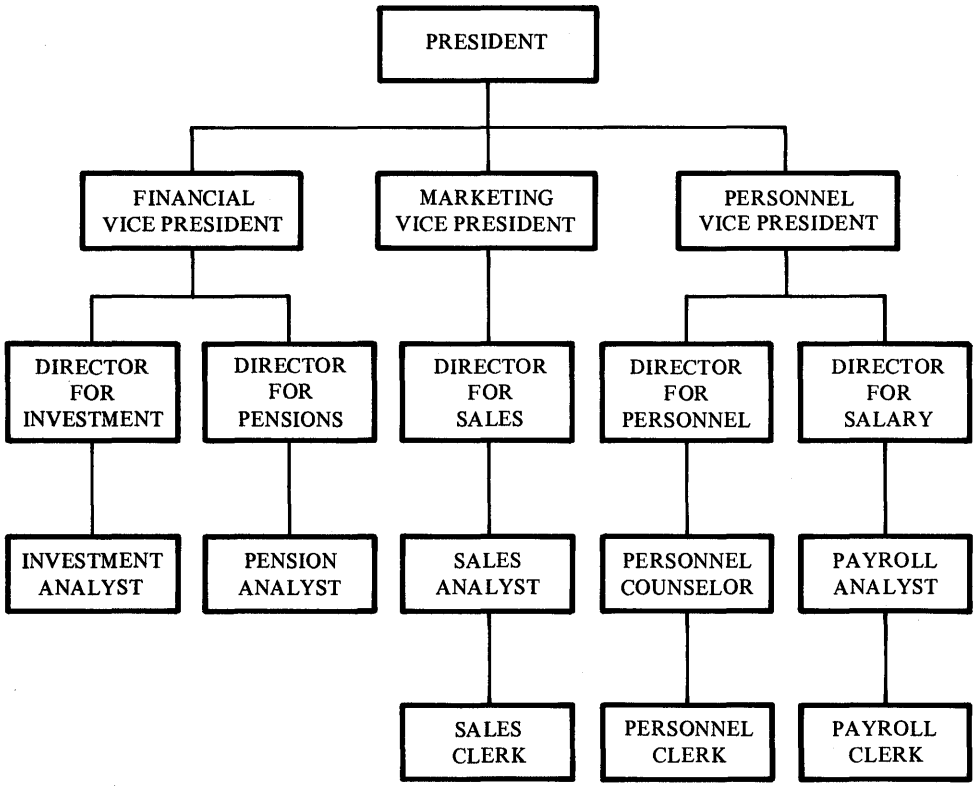

Figure 1. A Sample Corporate Structure

The president's authority pervades all levels in the organization. The president may access payroll records, sales reports, or employment records. Authority, however, does not move upward. The payroll clerk may not access the records of the financial vice president or of the investment department. And, authority is not lateral unless a higher authority allows it. The financial vice president may not normally access the organization's sales reports.

However, if the president needs a report of the organization's investments and determines that the sales records are essential to the report, the president may give the financial vice president access to the information while preparing the report.

RACF uses much the same structure as any organization. It allows an installation to define individuals and groups and what each individual or group may do. Some individuals and groups have a great degree of authority, while others have very little authority.

Your degree of authority is what you need to do your job. Your authorities may change with your job requirements. For example, you might not need to have a particular authority all the time but you might find it necessary for certain tasks. You may belong to a group with the needed authority and then drop from the group when your needs change.

RACF allows an organization to extend its structure to the protection of its information. However the organization arranges itself, it can also structure the protection of its information.

RACF follows the rule that most companies follow, that is, the rule of least possible privilege in controlling the use of information. The rule of least possible privilege is to give an individual all the authority necessary for his job but no unnecessary authority.

As mentioned in the previous example, the financial vice president has all the authority necessary to make decisions about his area, finance. To allow the financial vice president access to sales records would be a privilege above and beyond the job's requirements. Therefore, that authority would not generally be given to the financial vice president. RACF works the same way; it allows you to do your job but does not give you free run of information in the computer system.

An organization clearly defines the scope of the employee's job and identifies each employee uniquely. Each employee then becomes aware and responsible for what he or she has done or failed to do. RACF does the same. RACF is a security tool that uniquely identifies you and records what you do on the system. RACF uses user attributes, group authorities, and resource access authorities to control your use of the system.

RACF also keeps track of what is happening on the system so that an organization can determine what its employees are doing and if persons have attempted to perform unauthorized actions. The reports RACF produces act as a deterrent to unauthorized attempts to use information. Beyond that, RACF might also tell your organization if you need more information to do your job more effectively. If RACF reports that you consistently and unsuccessfully attempt to use a data set, the security administrator may find out why. You might need the information to do your work. Your security administrator can change your authority to meet your needs.

How RACF Protects

RACF is an access control facility that protects information by controlling access to the information. Information is one of an organization's major resources. RACF's premise is that you must have the proper authority to use protected information. RACF first asks who you are. RACF identifies you by means of a userid; a unique identification string. A userid, for example, may be a combination of your name, initials, personnel number, or department.

Once it knows who you are, RACF then requires you prove your identity. RACF verifies that you are the user you say you are by requesting and checking a password. When you are first defined to RACF, your group/security administrator assigns your userid and a temporary password. This temporary password permits initial entry to the system, at which time RACF requires you to supply a new password of your choice and known only to you. Unless you divulge it, no one knows this userid-password combination. In this way, RACF ensures personal accountability.

If RACF does not know you, RACF does not allow you to use RACF or any information it protects. It is as if there is a sentry at each checkpoint, and RACF is the sentry. If you are not known to RACF, RACF turns you away. If RACF knows you, it will ask you for a password to verify your identity. RACF then allows you to enter the system. Once you are in the system, RACF continually checks your clearances. Every time you approach a particular area, such as a protected data set, RACF checks your clearances to determine if they are proper for the particular area. If RACF clears you, you may enter the area, the data set. If you do not have proper clearance, RACF turns you away.

It is similar to the restrictions a organization places on its employees. One badge may give an employees access to the building but a second badge or a combination may be required for access to a restricted area such as the payroll department.

For example, in a bank, tellers may have access to the vault area but only officers of the bank may have the combination for the vault. The officers may be the only persons authorized to enter the vault.

User attributes, group authorities, and resource access authorities are the clearances RACF checks to determine who gets in and who does not. User attributes and group authorities describe users, while resource access authorities describe information.

Getting Ready To Use RACF

You may use RACF in two ways: with RACF commands and with the RACF ISPF panels. Both the commands and the panels allow you to do the same thing. To use the RACF ISPF panels, however, your organization must install additional program products. This book explains how to perform certain tasks using both RACF commands and RACF ISPF panels.

If your organization has the panels installed, the choice is yours. You may use either commands or panels to perform the tasks. If your organization has not installed the panels, you must use the commands to perform the tasks.

To use RACF, you must

- know how to conduct a TSO terminal session
- know how to use TSO commands
- be RACF-defined.

This book assumes that you are familiar with TSO. If you are not familiar with TSO, you will need to spend some time learning about a TSO terminal session and TSO commands before proceeding. See *TSO Terminal User's Guide* and *TSO Command Language Reference* for help.

Being RACF-Defined

Being RACF-defined is the starting point to using RACF. You may not define yourself to RACF. The security administrator defines new RACF users and permits them to use the system and certain protected resources. Resources not protected by RACF are generally accessible to anyone able to log on to the system.

When you are defined to RACF, your ability to use the system is defined at the same time. Your attributes are the operating privileges and restrictions assigned to you. Being RACF-defined is both making your identity known to RACF and describing your authority: what you may do and what resources you may use to perform those tasks.

About RACF Profiles

In an organization using RACF you will frequently hear the term profile. A profile in RACF is very much like your employee record at your organization. Your employee record describes you, including such things as date of employment, job title, salary, and ratings. RACF profiles do the same thing, but the information is RACF information.

The security administrator defines each authorized user, group, or resource. Users are the individuals in an organization. A group is a collection of individuals who have common needs or requirements. For example, the payroll department may be a group. A resource is the organization's information stored in its computer system, usually in data sets. In response to the security administrator's definition, RACF builds a description of the user, group, or resource. RACF's description is a profile. A profile is merely a file of descriptive information about a user, a group, or resource, such as a data set. RACF uses the information in a profile to control use of protected resources. When you attempt to use a protected resource, RACF checks your user profile as well as the resource profile to decide whether to allow you to use the resource.

User, group, and connect profiles describe individual users and groups, the people at an organization. Each user and group has a profile. Data set and general resource profiles describe the information and the levels of authority needed to use this information. A general resource is a resource other than a data set.

The security administrator or someone in authority in your organization is the one who controls the information in your user profile, in a group profile, or in a resource profile. You, as the end user, control the information in profiles describing your resources, your own data sets. You can change these profiles but you can not change the user or group profiles or other resource profiles. As a RACF user, you need to be familiar with the concept of profiles. The descriptions that follow are for your information. Don't let the terms confuse you and remember you do not control much of the information.

Generally, the security administrator decides the scope of a person's or group's authority and how a person or group uses a resource. Every RACF-defined user, group or resource has an owner. If you RACF-protect one of your own data

sets RACF designates you the owner. You could also be the owner of a group data set. Ownership implies responsibility for the group or resource. In most cases, the owner has full control over the group or resource.

There are five types of profiles:

- User profiles
- Group profiles
- Connect profiles
- Data set profiles
- General resource profiles

USER PROFILE

A user profile describes who you are and what you may do. It is a description of an individual using the computer system. The user profile contains:

- Information about your identity, such as your name and password.
- Your user attributes - your privileges within the system.
- The name of your default group. Every user is a member of at least one group. When you log on, if you belong to more than one group, RACF expects you to specify which group you wish have as your current connect group. If you do not specify a group, RACF assumes that your default group is your current connect group. You must have a default group if you belong to more than one group. If you belong to only one group, that group is your default group.
- The name of a model profile. This profile is a sample for new profiles.
- How often you must change your password.

GROUP PROFILE

A group profile describes a group of users defined together because of their common needs. For example, a group may be all the secretaries in a particular department. The group profile contains:

- Information about the group, such as the group's owner, its superior group and its subgroups. A superior group could be the group of administrative assistants to whom the secretaries report. A subgroup may be the group of clerks who report to the secretaries.
- A list of connected users. The connected users have the privileges of the group while connected to the group.
- The group authorities of the members of the group.

CONNECT PROFILE

A connect profile describes a user's relationship to the group. Each RACF user has a connect profile for each group that he or she is connected to. RACF connects you to either a group you specify or to your default group. You will be connected to only one group at a time.

Being connected to a group allows you privileges within the group. Being connected is making you part of a group that you would not normally be part of. For example, temporarily assigning you to supervise a group other than your own so that the clerks in that group may assist you with a heavy workload. In RACF, connecting you to another group allows you to use their data sets or other resources. An advantage of being connected to a particular group is that you might need authority the group has to perform a job. For most of your work, your only concern is your own user attributes and the protection of your resources, your data sets.

The connect profile contains:

- The profile owner's name.
- Connect (group-level) attributes - Your user privileges when associated with this group.
- Other information about the group.

RESOURCE PROFILE

RACF maintains two types of resource profile:

- **data set profiles**
- **general resource profiles**

Data set profiles contain security information about DASD data sets, while general resource profiles contain security information about resources other than DASD data sets. The resource profile contains:

- The resource name.
- The resource owner.
- The access list - a list describing who may use a resource and how they may use the resource.
- The universal access authority (UACC) - the default level of access authority allowed for all users not listed in the access list.
- Auditing information - RACF can audit the use of each resource. The audit can be general or very specific. For example, you can set up a resource profile for your data set to audit every attempt to use the data set. Or, you define the profile to audit only the attempts to update the data set.

In addition, a data set profile contains the volume serial number while a general resource profile contains the class name that tells you the type of resource it is.

There are two types of data set and general resource profiles. One is a discrete profile, the other is a generic profile.

A discrete profile protects a single resource, such as a sensitive data set that has unique security requirements. It contains a description of the data set, including the authorized users, the access authority of each user, and the location of the data set.

A generic profile protects several resources that have a similar naming structure and security requirements. It is like an umbrella; you may protect many resources with similar characteristics with a generic profile. Two advantages to a generic profile are that resources protected by a generic profile do not have to be individually defined to RACF and the generic profile protects all copies of the resources on all volumes in all locations in the system.

A generic profile is similar to a discrete profile, except that when you define the profile, you include one or more generic characters (% or *) in the data set name or you specify the profile as a generic profile.

For example, assume you are creating a generic profile for a series of data sets containing video games. You would create the profile with the name: "USERID.GAMES.*." All data set names beginning with USERID.GAMES would be protected.

HOW RACF DETERMINES WHAT YOU CAN DO

There are three factors that determine how you can use RACF. They are:

- your user and connect attributes.
- group authorities.
- resource access authorities.

With RACF, user and connect attributes, group authorities, and resource access authorities control your use of the system and its protected resources. RACF allows you to do your job while still protecting the company's resources.

User attributes and group authorities describe individual users and groups. You, as an end user, need to understand how these attributes and authorities affect you and your ability to do your job. However, resource access authorities may concern you the most. Resource access authorities determine how you can use information on the system. In most instances, your concern is protecting your information and using whatever information you need for your job.

User and Connect Attributes

You may have attributes at either the system level or at the group level. Attributes specified at the system level are user attributes, while attributes specified at the group level are connect or group attributes. If you have a user attribute, the user attribute overrides any connect (group-level) attribute. If you have a user attribute, it applies across the system, to all groups, even if it is not specified at the group level. A connect (group-level) attribute specified for a group applies only to that group and to the resources and users owned by that group.

As an end user, you may not have any of the user or connect (group-level) attributes listed below and you will still be able to use RACF. In fact, most attributes actually allow you extraordinary privileges and generally only a few individuals have these attributes.

The possible user and connect attributes are:

- SPECIAL
- AUDITOR
- OPERATIONS

- GRPACC
- ADSP
- REVOKE
- CLAUTH, a user attribute that cannot be a connect (group-level) attribute.
- NONE (no assigned attributes)

The SPECIAL attribute gives you full control over the RACF profiles on the RACF data set and allows you to issue all RACF commands. It may be a user or a connect (group-level) attribute.

The AUDITOR attribute allows you to audit the security controls and system resources and create security reports. It may be a user or a connect (group-level) attribute.

The OPERATIONS attribute allows you to perform any maintenance operations, such as copying, reorganizing, cataloging, and scratching a RACF-protected resource. It may be a user or a connect (group-level) attribute.

The GRPACC attribute allows you to have the group data sets you allocate automatically accessible to other users in the specified group. However, you must protect the data set with a discrete profile. It may be a user or a connect (group-level) attribute.

The ADSP attribute automatically protects all of your permanent DASD data sets with discrete profiles. It may be a user or a connect (group-level) attribute. ADSP is the automatic data set protection attribute. You cannot forget to protect a data set; RACF does it for you.

The REVOKE attribute allows you to exclude a RACF-defined user from entering the system. It may be a user or a connect (group-level) attribute.

The CLAUTH attribute allows you to define profiles for any class specified in the class name. You may have this attribute only at the system level. It may only be a user attribute.

As an end user, you may have ADSP, but it is unlikely that you would have any of the other attributes. In fact, when you list your attributes (Task 1 tells you how to do this.) the attribute field may have the word NONE. NONE does not mean you cannot do work. What it means is that you do not have any of the user or connect attributes, which actually provide extraordinary capabilities within the system.

Group Authorities

Group authorities define your responsibilities within the group. If you have a group authority, it applies to the specified group only. A group authority does not have the scope of a user attribute. A user attribute applies to you across the system, while a group authority applies only within the confines of the group. This is not to say that the authority is not powerful. Depending on the group and its resources, the authority could be extensive.

The possible group authorities are:

- USE - allows you to enter the system under the control of the specified group. You may use any of the resources the group may use.
- CREATE - allows you to RACF-protect a group data set and control who can access the data set. It includes the privileges of the USE authority.
- CONNECT - allows you to connect RACF-defined users to the specified group and assign these users the USE, CREATE, or CONNECT authority. It includes the privileges of the CREATE authority.
- JOIN - allows you to define new users or groups to RACF and to assign group authorities. To define new users, you must also have the user attribute, CLAUTH. JOIN authority includes all the privileges of the CONNECT authority.

Every RACF user will belong to at least one group and have at least one group authority. RACF uses the concepts of groups and ownership to establish control. The concept of groups and ownership in RACF is not any different than in any organization. The higher a person or group in the organization the more control and authority the individual or group will have.

Figure 2 illustrates a group structure showing which resources you may use and which you may not use.

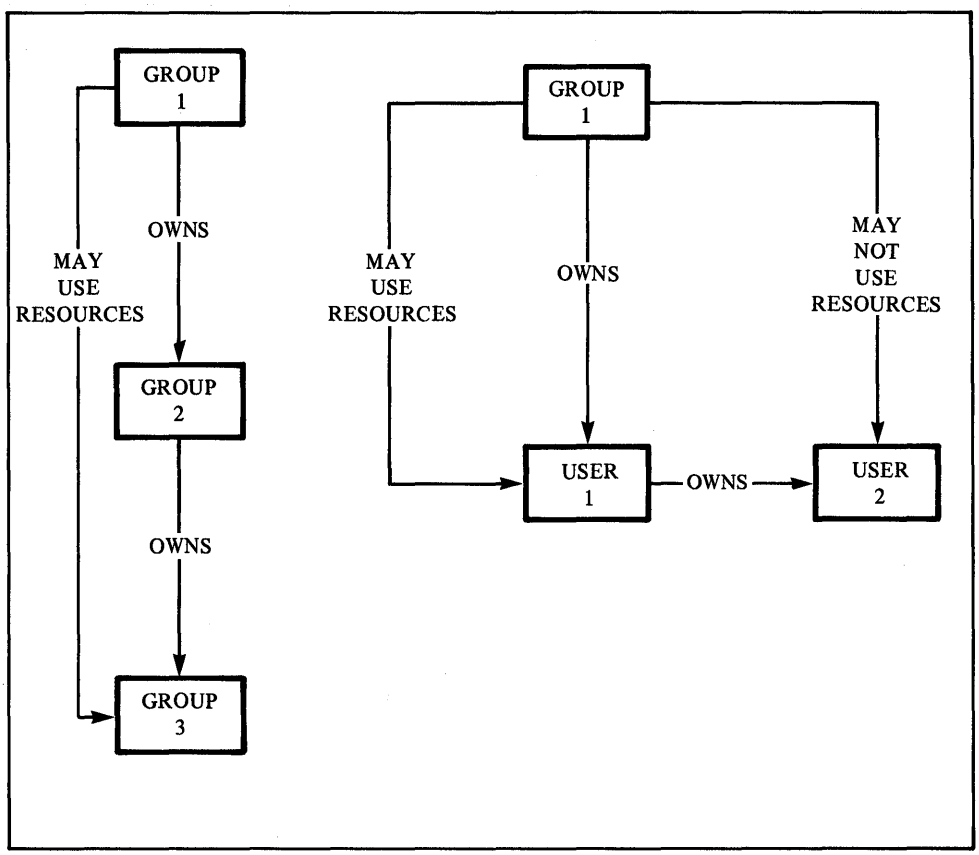

Figure 2. Group Structure

Resource Access Authorities

RACF can explicitly grant or deny you access to a resource by assigning each user or group a specific access authority. RACF controls in two ways, both equally important. RACF controls **who** may access protected resources and **how** they may access the resource.

The possible resource access authorities are:

- ALTER - gives you full control to authorize other users or groups to access the resource. It also gives you the ability to rename or scratch the data set. It is the highest authority.
- CONTROL - gives you authority equivalent to the VSAM control password.
- UPDATE - allows you to access the resource to read or write to it. UPDATE gives you less control than ALTER but more than READ.

- READ - allows you to access the resource to read only.
- NONE - prevents you from accessing the resource.

In addition to the specific resource access authorities, each resource has the default access authority, UACC. UACC is the universal access authority; it defines the default access authority. All users or groups not specifically named in a resource profile can still use the resource with the authority specified in UACC. For example, assume the profile for the ABC data set does not name J.E.Smith as an authorized user. If, however, the ABC data set profile lists the UACC as READ, J.E. Smith may read the ABC data set.

GETTING STARTED

Task 1 allows you to gather information rather than perform a specific task. You will frequently need to know what your capabilities are before you will be able to perform a specific task. Being defined to RACF is the starting point to using RACF.

Task 1. Finding Out If You Are RACF-Defined

SITUATION: Your first step is to find out if you can use RACF. As a starting point, you must find out if you have been RACF-defined.

There are two procedures to find out if you're defined to RACF, one is for TSO/E users and the other is for non-TSO/E users. If you are not sure whether your installation has installed TSO/E, use the procedure for non-TSO/E users.

> Be aware, if this is the first time you have ever logged on to the system, that you must change your password. After you have entered your assigned temporary password, you will receive a message saying that it has expired. Enter a new password of your choice, following the format of the assigned password.

For TSO/E Users: Log on to the system. Simply observe the right side of your logon parameter screen. If the NEW PASSWORD and GROUP IDENT fields appear, you are a RACF-defined user.

The following is an example of a screen for a TSO/E user:

```
ENTER LOGON PARAMETERS BELOW:      RACF LOGON PARAMETERS:

USERID       ======> ABCXYZ1

PASSWORD     ======>               NEW PASSWORD  =====>

PROCEDURE    ======> PROCO1        GROUP IDENT   =====>

ACCT NMBR    ======> A4446B

SIZE         ======>

PERFORM      ======>

COMMAND      ======>
```

For Non-TSO/E Users: Log on to the system by entering your userid. If you are not aware that you have a userid, see your group/security administrator or someone in authority at your installation, for example, a supervisor. Without a userid you cannot use the system.

Issue the LISTUSER command, type:

LISTUSER

If you are not a RACF-defined user, you will get a command-violation message. A command-violation message indicates you are not authorized to issue this command.

If you discover that you are not RACF-defined, contact your group/security administrator or someone in authority at your installation, for example, a supervisor. You must be RACF-defined to use RACF.

If you are a RACF-defined user, you will see a screen similar to the one shown.

This portion of the screen describes you as the user.

```
USER=your    NAME=your     OWNER=your    CREATED=date you
     userid       name           owner           were
                                                 defined
                                                 to RACF


DEFAULT-GROUP=your    PASSDATE=date  PASS-INTERVAL=length of
           default     your password               time your
         group name    was last updated            password
                                                   is valid


ATTRIBUTES=your operating privileges and restrictions


LAST-ACCESS=last date you were on the system


CLASS-AUTHORIZATIONS=installation assigned classes in which
                     the user can define profiles.


INSTALLATION-DATA=information your installation maintains
                  about you


MODEL-NAME=a profile used as a model for new data set
profiles
```

This portion of the screen describes the group(s) you belong to and what you can do as a member of the group(s).

```
GROUP=name AUTH=your CONNECT-OWNER=your CONNECT-DATE=date
      of        group               group        you were
      group     authority           owner        connected
                                                 to group


CONNECTS=number    UACC=universal     LAST-CONNECT=last time
       of times          access                  you were
       you were        authority                 connected
      connected
       to group


CONNECT ATTRIBUTES=your operating privileges
                   as a member of the group
```

Here are brief descriptions of the terms appearing on the screen:

USER =

Your userid is the name the system knows you by. It is frequently a combination of such identifying information as your name, initials, personnel number, or department.

OWNER =

Each RACF-defined user has a user profile. A user profile is a description of who you are and what you can do. Each user profile has another RACF user (an individual or a group) as its owner. Your owner may modify your profile.

CREATED =

The date you first became known to RACF (RACF-defined).

DEFAULT-GROUP =

RACF connects each user to at least one group. If you are connected to only one group, that group is your default group and that group name appears in this field. If you are connected to more than one group, at logon you specify the group you want to be connected to. If you don't specify the group, RACF assumes the group named in this field.

PASSDATE =

The date you last updated your password.

PASS-INTERVAL =

The length of time in days your current password is valid. You must change your password before this interval expires.

ATTRIBUTES =

The operating privileges and restrictions assigned to you. There are two types of attributes: user and connect. User attributes are attributes that apply to you all the time and in all areas of the system. Connect attributes apply to a specified group. The possible attributes are:

SPECIAL
AUDITOR
OPERATIONS
GRPACC
CLAUTH
ADSP
REVOKE

See "How RACF Determines What You Can Do" for a definition of each of these attributes. You may also see NONE in this field. NONE indicates you do not have any user attributes, though you can still use RACF. In fact, most attributes actually allow you extraordinary privileges, and generally only a few individuals or groups have these attributes.

LAST-ACCESS =

The date is the last time you were on the on the system. RACF keeps records of all persons who have used the system, and what they have done, as well as recording unauthorized attempts to use of the system.

CLASS-AUTHORIZATIONS =
Your installation assigns resources to various classes. The class appearing in this field is the class in which the user is authorized to assign RACF protection.

INSTALLATION-DATA =
Additional information your installation maintains about you and your authority. If you need help to understand anything included here, check with your group/security administrator or owner.

MODEL-NAME =
A profile used as a model for new data set profiles.

GROUP =
The name of the group to which you are connected.

AUTH =
These are authorizations that apply to the group to which you are connected. The four group authorities, listed in lowest to highest order, are:

USE
CREATE
CONNECT
JOIN

Every RACF user has a group authority. The authorities are hierarchical in that a higher authority includes the capabilities of a lower authority.

CONNECT-OWNER =
The name of the owner of the group to which you are connected.

CONNECT-DATE =
The date you were first connected to the group specified in the field, group name.

CONNECTS =
The number of times you were connected to the group.

UACC =
The universal access authority for resources you create while connected to this group. If a user is not specifically listed in the access list describing a resource owned by the connect group, RACF looks at UACC and allows the user to use the resource in the manner specified in the UACC. The UACC may be:

ALTER
CONTROL
UPDATE
READ
NONE

See "How RACF Determines What You Can Do" for a definition of each of these attributes.

LAST-CONNECT =
The last time you were connected to the group.

CONNECT-ATTRIBUTES =
The operating privileges and restrictions assigned to you when you are connected to the group. Connect attributes may also be called group-level attributes. The possible connect (group-level) attributes are:

SPECIAL
AUDITOR
OPERATIONS
GRPACC
ADSP
REVOKE

See "How RACF Determines What You Can Do" for a definition of each of these attributes. You may also see NONE in this field. NONE indicates you do not have any connect attributes, though you can still use RACF. In fact, most attributes actually allow you extraordinary privileges and generally only a few individuals or groups have these attributes.

This example shows an actual screen describing a RACF user connected to only one group.

```
USER=SMITH    NAME=J.E.SMITH    OWNER=JONES    CREATED=84.096

DEFAULT-GROUP=DEPTD60    PASSDATE=84.103   PASS-INTERVAL= 30

ATTRIBUTES=NONE

LAST-ACCESS=84.114/13:47:18

CLASS AUTHORIZATIONS=NONE

NO-INSTALLATION-DATA

NO-MODEL-NAME

GROUP=DEPTD60   AUTH=USE   CONNECT-OWNER=JONES   CONNECT-DATE=84.096

 CONNECTS= 05    UACC=NONE    LAST-CONNECT=84.114/13:47:18

   CONNECT ATTRIBUTES=NONE
```

In this example user, J.E. Smith has none of the possible user attributes. He is still able to use RACF; he can, for example, create data sets and RACF-protect them.

If you find that you are unable to perform a certain task adequately because you are not connected to the necessary group(s) or your authority is not sufficient, contact your group/security administrator or owner.

This example shows an actual screen describing a RACF user connected to two groups with different authority within each group.

```
USER=SMITH   NAME=J.E.SMITH   OWNER=JONES  CREATED=84.096
DEFAULT-GROUP=SEARCH  PASSDATE=84.103   PASS-INTERVAL= 30
ATTRIBUTES=ADSP
LAST-ACCESS=84.114/13:47:18
CLASS AUTHORIZATIONS=NONE
NO-INSTALLATION-DATA
MODEL-NAME=SMITH.MODEL
GROUP=SEARCH AUTH=JOIN CONNECT-OWNER=WILL CONNECT-DATE=84.096
   CONNECTS= 01   UACC=NONE   LAST-CONNECT=84.114/13:50:18
   CONNECT ATTRIBUTES=NONE
GROUP=PAYROLL AUTH=CREATE CONNECT-OWNER=MILL CONNECT-DATE=84.096
   CONNECTS= 00  UACC=READ  LAST-CONNECT=84.114/13:55:18
   CONNECT ATTRIBUTES=NONE
```

In this example, user, J.E. Smith has the ADSP user attribute. A user attribute overrides any connect (group-level) attribute. If you have a more powerful attribute as a user, it takes precedent over a lesser connect (group-level) attribute. What you can do as a user, you can do as a member of a group. With the ADSP attribute, RACF automatically protects all of Smith's permanent data sets. Smith also has a model data set profile, so whenever Smith creates a permanent data set, RACF uses the name of the data set appearing in the MODEL-NAME as a model for the new data set profile.

Smith also belongs to two different groups, SEARCH and PAYROLL. In the SEARCH group, Smith can assign group authorities to members of the group. In the PAYROLL group, Smith can RACF-protect a data set and decide who can use the data set.

In the PAYROLL group, Smith also has assigned a UACC of READ. UACC stands for universal access authority. Any user not specifically mentioned in the access list describing a resource, may use the resource in the manner specified in the UACC. Thus, when Smith defines a PAYROLL data set, the UACC is set to READ unless Smith sets the the UACC to another value. All RACF-defined users have read only access to the data set.

PROTECTING YOUR INFORMATION USING RACF COMMANDS

Tasks 2 through 14 tell you how to protect your information using RACF commands.

If you are an infrequent user of RACF, you may want to review Task 1 to get you started.

In each task there is a short description of a situation which sets the stage as an example of why you might want to perform the task.

Task 2. Finding Out What Authority You Have

SITUATION: You must protect a sensitive data set using RACF but you are not aware of what you can do using RACF.

To find out what you can do using RACF, issue the LISTUSER command. Type:

LISTUSER

You will see a screen similar to the screen shown that displays the contents of your profile.

Your owner/administrator creates and maintains your user profile, which describes you to RACF. Your profile contains: your owner's name, your userid, information about your operating privileges and restrictions, information about your default group and other groups to which you belong, and other important information.

If, after determining what your operating privileges and restrictions are, you need to change your user profile. See your group/ security administrator or owner.

This screen displays the contents of a user profile.

This portion of the screen describes you as the user.

```
USER=your    NAME=your     OWNER=your    CREATED=date you
     userid       name           owner           were
                                                 defined
                                                 to RACF


DEFAULT-GROUP=your    PASSDATE=date  PASS-INTERVAL=length of
           default     your password               time your
         group name    was last updated           password
                                                   is valid


ATTRIBUTES=your operating privileges and restrictions


LAST-ACCESS=last date you were on the system


CLASS-AUTHORIZATIONS=installation assigned classes in which
                     the user can define profiles.


INSTALLATION-DATA=information your installation maintains
                  about you


MODEL-NAME=a profile used as a model for new data set
profiles
```

This portion of the screen describes group(s) you belong to and what you can do as a member of the group(s).

```
GROUP=name AUTH=your CONNECT-OWNER=your CONNECT-DATE=date
      of        group               group        you were
      group     authority           owner        connected
                                                 to group


CONNECTS=number    UACC=universal    LAST-CONNECT=last time
       of times          access                  you were
       you were        authority                 connected
      connected
       to group

CONNECT ATTRIBUTES=your operating privileges
                   as a member of the group
```

For a detailed description of the terms in this screen and examples of actual screens, see Task 1.

Task 3. Finding Out What Profiles You Have

SITUATION: You created a data set that needs protection, but you do not know whether you currently have a profile that will protect the data set.

To find out what profiles you have, issue the SEARCH command. Type:

SEARCH

RACF will list all your profiles. If you do not have any profiles, RACF will display a message telling you that there are no profiles.

Task 4. Changing Your Password

SITUATION: You suspect that your password has become known to others. Or, perhaps you would prefer to change your password more frequently than your installation requires.

In choosing a new password, be aware that your installation has password rules. If you do not know the rules, choose a password following the format of your current password. RACF may not allow you to re-use a previous password. See your group/security administrator or owner for an explanation of your installation's rules for passwords.

To change your password, issue the PASSWORD command with the PASSWORD keyword. Type:

PASSWORD PASSWORD(current password new password)

For example, to change your password from "subject" to "testers," type:

PASSWORD PASSWORD(subject testers)

To change your password interval, issue the PASSWORD command with the INTERVAL keyword. Type:

PASSWORD INTERVAL(interval you want)

For example, to change your password interval to 15 days, type:

PASSWORD INTERVAL(15)

RACF allows the interval to be in the range of 1 to 254 days. Your installation chooses its own interval in this range. You can change your password interval to be a shorter length of time than your installation requires but you cannot specify a longer interval. For example, if your installation has a password interval of 30 days, you may change the interval to any number from 1 to 30 but you cannot change your password interval to 45 days.

To change your password and password interval, issue the PASSWORD command with the PASSWORD and INTERVAL keywords. Type:

PASSWORD PASSWORD(current password new password) INTERVAL(interval)

For example, to change the password from "subject" to "testers" and the interval to 15 days, type:

PASSWORD PASSWORD(subject testers) INTERVAL(15)

If you don't know what your current password interval is, issue the LISTUSER command and check the PASS-INTERVAL field. See Task 1 if you need more information.

You may also change your password while logging on to the system. See Task 1.

Task 5. Finding Out How a Data Set is Protected

SITUATION: Suppose you want to restrict a data set to only a few people, but you are not aware of the current status of the data set.

To determine the status of a data set, issue the LISTDSD command. Type:

LISTDSD DATASET('profile name') ALL,

For a discrete profile, the profile name and data set name are the same.

If the command fails, you will get a message stating you are not authorized. See your group/security administrator or owner.

If the command succeeds, you will see a listing of the profile, similar to the following screen.

```
 LEVEL        OWNER          UNIVERSAL ACCESS     WARNING
 -----        -----          ----------------     -------
  00          SMITH               READ              NO

  AUDITING
 ----------
  SUCCESS(UPDATE)

  YOUR ACCESS          CREATION GROUP         DATASET TYPE
--------------       ----------------       --------------
   READ                   DEPTD60               NON-VSAM

 VOLUMES ON WHICH DATASET RESIDES              UNIT
----------+-------------------------          ------
           21345                              SYSDA

INSTALLATION DATA
-------------------
PL/1 LINK LIBRARY

CREATION DATE      LAST REFERENCE DATE      LAST CHANGE DATE
(DAY)  (YEAR)       (DAY)      (YEAR)        (DAY)   (YEAR)
-------------      ------------------       ---------------
 070    85           070        85             070     85

ALTER COUNT     CONTROL COUNT     UPDATE COUNT     READ COUNT
-----------     -------------     ------------     ----------
 00000            00000             00002           00000

USER          ACCESS               ACCESS COUNT
----          --------             --------------
JONES         UPDATE                 00009
  *             *                      *
```

Check the following fields for the most important security information about how the data set is protected:

- the OWNER field
- the UACC field
- the USER field
- the ACCESS field

Here are brief descriptions of the fields appearing on the screen:

LEVEL
An indicator used by each individual installation. If anything other than 00 appears in this field, see your group/security administrator or owner for an explanation of what the number means.

OWNER
Each RACF-defined data set has an owner. An owner may be an individual or a group. When you create a data set and then RACF-protect the data set without specifying an owner, RACF names you the owner of the data set profile. The owner of the profile may modify the data set profile.

UNIVERSAL ACCESS
Each data set protected by RACF has a universal access authority (UACC). The UACC permits individuals or groups to use the data set in the manner specified in this field. In this example, the UACC is READ. Anyone may read this data set. (The only exception is if the individual is specifically named in the access list with a UACC of NONE.)

WARNING
If this field contains YES, RACF permits a user to access this resource even though his/her access authority is insufficient and will issue a warning message describing this condition. If this field contains NO, RACF does not permit a user with insufficient authority to access this resource.

AUDITING
The type of access attempts that are recorded. In this example, the AUDITING is SUCCESS (UPDATE). RACF will record all successful attempts to update the data set.

YOUR ACCESS
How you may access this data set. If NONE appears in this field, you are not in the access list.

CREATION GROUP
The group under which the profile was created.

DATASET TYPE
The data set type. It may be either VSAM or non-VSAM.

VOLUME ON WHICH THE DATASET RESIDES
The volume on which a non-VSAM data set resides or the volume on which the catalog for a VSAM data set resides.

UNIT
The unit type on for a non-VSAM data set

INSTALLATION DATA
Any information your installation keeps in this data set profile.

CREATION DATE
The date the profile was created.

LAST REFERENCE DATE
The last time the profile was accessed.

LAST CHANGE DATE
The last time the profile was changed.

ALTER COUNT
The number of times the profile was altered.

CONTROL COUNT
The number of times the profile was successfully accessed with CONTROL authority.

UPDATE COUNT
The number of times the profile was successfully accessed with UPDATE authority.

READ COUNT
The number of times the profile was successfully accessed with READ authority.

USER
Any specific users or groups permitted access to the data set.

ACCESS
How any users listed in the USER field accessed the data.

ACCESS COUNT
The number of times any users listed in the USER field accessed the data set.

If you must work with the listed data set but do not have the required authority, get in touch with the owner and have him/her issue a PERMIT command to give you access to the data set.

Task 6. Changing A Data Set's Access Authority (UACC)

SITUATION: You have a data set containing research data. There is a need to protect the information so that no one can tamper with the experimental data.

To change a data set's UACC, requires the ALTDSD command. Use of this command requires certain authority. As an end user, in most probability, the only condition that you will meet is that you are the owner of the profile. STEP 1 tells you how to determine if you own the profile. If you know you are the owner, proceed with STEP 2.

STEP 1. Determining the current universal access authority (UACC) of the data set and the profile owner

To find out the current UACC and the profile owner, issue the LISTDSD command. Type:

LISTDSD DATASET('profile name') ALL

If the command fails, you will get a message stating you are not authorized. See your group/security administrator or owner.

If the command succeeds, you get a listing of the profile. Check the OWNER field for the current owner, the UACC field for the current access authority, and the USER ACCESS fields.

If you are not the owner or you are not listed in the access list, you cannot change the UACC. If you need more information on the data set profile, see Task 5.

STEP 2. Changing the universal access authority (UACC)

To change the UACC, issue the ALTDSD command. Type:

ALTDSD 'profile name' UACC(level)

The UACC can be only one of the following:

NONE
no access to the data set

READ
read only access to the data set

UPDATE
read and write access to the data set

CONTROL
VSAM control password access to VSAM data set

ALTER
full control of the resource profile for the data set

CAUTION

Anyone who has READ authority (or UPDATE, CONTROL, or ALTER) to your protected user data set can create a copy of it. As owner of the copied data set, that user has control of the security level of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See Task 10 for information on how to permit selected users or groups to access a data set.

For Example:

To change the UACC for the user data set, USERID.PROJ.ONE, to NONE, type:

ALTDSD 'USERID.PROJ.ONE' UACC(NONE)

To change the UACC for the group data set, GROUPID.PROJ.ONE, to READ, type:

ALTDSD 'GROUPID.PROJ.ONE' UACC(READ)

To change the UACC for the generic profile, USERID.*, to NONE, type:

ALTDSD 'USERID.*' UACC(NONE)

To change the UACC for the generic profile, USERID.PROJ.*, to NONE, type:

ALTDSD 'USERID.PROJ.*' UACC(NONE)

Remember changing the UACC for a generic profile changes the access to all data sets protected by the profile.

If the command fails, you will get a message stating you are not authorized. See your group/security administrator or owner.

CAUTION

If you are changing the UACC to restrict access, be certain that any individual or group specifically mentioned in the access list has the access to the resource that you intend. If you change the UACC to NONE and have a user specifically named in the access list with ALTER authority, that user will have ALTER authority to the resource.

Conditions for using ALTDSD command: RACF requires one of the following conditions be met:

- You have the SPECIAL user attribute (see Task 2).
- You have the SPECIAL connect attribute (see Task 2) and the data set is within the scope of the group in which you have the SPECIAL connect attribute.
- You own the data set.
- Your userid is the high-level qualifier of the profile name.
- If you are changing the UACC of a data set protected by a discrete profile, you are on the access list with ALTER authority, (see STEP 1).
- If you are changing the UACC of a data set protected by a discrete profile, your current connect group is on the access list with ALTER authority (see STEP 1).
- The UACC is ALTER (see STEP 1).

Task 7. Changing A Data Set's Audit Type

SITUATION: You would like tighter control over a particular data set. You want to know about all attempts to use the data set.

To change a data set's audit type requires the ALTDSD command. Use of this command requires certain authority. As an end user, in most probability, the only condition that you will meet is that you are the owner of the data set profile. If you know that you are the owner, proceed with STEP 2. STEP 1 tells you how to determine if you own the data set profile.

STEP 1. Determining the current audit type and the profile owner

To find out the audit type and profile owner, issue the LISTDSD command. Type:

LISTDSD DATASET('profile name') ALL

If the command fails, you will get a message stating you are not authorized. See your group/security administrator or owner.

If the command succeeds, you get a listing of the profile. Check the AUDITING field for the current audit type. If you need more information on the data set profile, see Task 5.

STEP 2. Changing the audit type

To change the audit type, issue the ALTDSD command. Type:

ALTDSD 'profile name ' AUDIT(type (level))

The audit type which specifies the access attempts you want recorded, can be only one of the following and must be entered:

ALL
records all attempts to access the data set

FAILURES
records all unauthorized attempts to access the data set

SUCCESS
records all authorized attempts to access the data set

NONE
no recording

An optional parameter, the audit access level is the access level at which someone attempted to access a protected resource. It can be:

READ
records attempts at any level

UPDATE
records attempts to update a data set

CONTROL
records attempts to update a VSAM data set

ALTER
records attempts to alter the data set

default =
READ

If the command fails, you will get a message stating you are not authorized. See your group/security administrator or owner.

For Example:

To change the audit type of the data set, USERID.PROJ.ONE, to ALL and the audit access level to ALTER, type:

ALTDSD 'USERID.PROJ.ONE' AUDIT(ALL(ALTER))

To change the audit type of the data set, USERID.PROJ.ONE, to ALL, type:

ALTDSD 'USERID.PROJ.ONE' AUDIT(SUCCESS)

The result will be that USERID.PROJ.ONE will have an audit type of SUCCESS and an audit access level of READ. (READ is the default if you do not specify the audit access level.)

To change the audit type of the group data set, GROUPID.PROJ.ONE, to ALL and the audit access level to ALTER, type:

ALTDSD 'GROUPID.PROJ.ONE' AUDIT(ALL(ALTER))

To change the audit type of the group data set, GROUPID.PROJ.ONE, to ALL, type:

ALTDSD 'GROUPID.PROJ.ONE' AUDIT(ALL)

The result will be that GROUPID.PROJ.ONE will have an audit type of ALL and an audit access level of READ. (READ is the default if you do not specify the audit access level.)

To change the audit type for the generic profile, USERID.*, to ALL and the audit access level to ALTER, type:

ALTDSD 'USERID.*' AUDIT(ALL(ALTER))

Remember changing the audit type for a generic profile changes the audit type for all data sets protected by the profile.

Conditions for using ALTDSD command: RACF requires one of the following conditions be met:

- You have the SPECIAL user attribute (see Task 2).
- You have the SPECIAL connect attribute (see Task 2) and the data set is within the scope of the group in which you have the SPECIAL connect attribute.
- You own the data set.
- Your userid is the high-level qualifier of the profile name.
- If a data set is protected by a discrete profile, you are on the access list with ALTER authority, (see STEP 1).
- If a data set is protected by a discrete profile, your current connect group is on the access list with ALTER authority (see STEP 1).
- The UACC is ALTER (see STEP 1).

Task 8. Creating A Discrete Profile To Protect A Data Set

SITUATION: You have a single data set that need to be protected with very specific requirements or one of your more sensitive user data sets is not currently protected.

In either case, you will create a *discrete profile* for the data set to establish the unique access characteristics you want. When you create a profile, either discrete or generic, you are establishing RACF protection for a data set.

To create a discrete profile, you must be defined to RACF and have the authority to issue the ADDSD command. To find out if you are defined, see Task 1. If you are RACF-defined, proceed with the task.

If you have the ADSP (automatic data set protection) attribute assigned to you at the user level, every user or group data set you create is automatically protected. If the ADSP attribute is assigned to you at the group level, every user or group data set you create while logged on under that group is automatically protected. To check if you have the ADSP attribute, see Task 1.

To create a discrete profile for a cataloged data set, issue the ADDSD command. Type:

ADDSD 'data set name' UACC(level) AUDIT(type (level))

To create a discrete profile for a data set that is not cataloged, issue the ADDSD command. Type:

ADDSD 'data set name' UNIT(type) VOLUME(volume-serial)
UACC(level) AUDIT(type (level))

If you are creating a profile to protect a data set that is not cataloged, RACF must know the unit type and the volume serial number where the data set resides.

The UACC can be only one of the following:

NONE
no access to the data set

READ
read only access to the data set

UPDATE
read and write access to the data set

CONTROL
VSAM control password access to VSAM data set

ALTER
full control of the resource profile for the data set

default =
the value specified in the UACC field in your current connect group. See Task 1 for more information.)

CAUTION

Anyone who has READ authority (or UPDATE, CONTROL, or ALTER) to your protected user data set can create a copy of it. As owner of the copied data set, that user has control of the security level of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. See Task 10 for information on how to permit selected users or groups to access a data set.

The audit type which the access attempts you want recorded, can be only one of the following and must be entered:

ALL
records all attempts to access the data set

FAILURES
records all unauthorized attempts to access the data set

SUCCESS
records all authorized attempts to access the data set

NONE
no recording

default =
FAILURES

An optional parameter, the audit access level is the access level at which someone attempted to access a protected resource. It can be:

READ
records attempts at any level

UPDATE
records attempts to update a data set

CONTROL
records attempts to update a VSAM data set

ALTER
records attempts to alter the data set

default =
READ

For Example:

To create a discrete profile for the user data set, SMITH.PROJ.ONE. Type:

ADDSD 'SMITH.PROJ.ONE' UACC(READ) AUDIT(ALL)

To create a discrete profile for the group data set, GROUPID.PROJ.ONE. Type:

ADDSD 'GROUPID.PROJ.ONE' UACC(READ) AUDIT(ALL)

For a discrete profile the profile name and data set name are the same.

CAUTION

If your installation is an "always-call" installation (that is, RACF is always called each time an attempt is made to access a data set or general resource), keep in mind the that a generic profile might already exist under which the data set might be protected. But the profile might not possess the exact access control information you want for your data set. In this case, you can create a more specific generic profile or a discrete profile for the data set.

To find out if you are in an always call environment, ask your group/security administrator or owner.

Task 9. Creating A Generic Profile To Protect Data Sets

SITUATION: You have several data sets that have similar security requirements.

For general use you can create a *generic profile* rather than a discrete profile and then selectively permit each user or group access to the data. When you create a profile, either discrete or generic, you are establishing RACF protection for a data set.

For a generic profile, the unit and volume information is ignored because the data sets that are protected under the generic profile might be on many different volumes. Further, when a data set that is protected by a generic profile is scratched, the profile remains intact (unlike a discrete profile).

To create a generic profile for your user data set, the high-level qualifier must be your userid.

To create a generic profile for a group data set, you must have either the SPECIAL attribute at the user or group level or CREATE authority in the group. If you need more information on your attributes or authorities, see Task 1.

You create a generic profile in the same manner as a discrete profile, except that you include one or more generic characters (% or *) in the profile name you specify with the ADDSD command or you include the GENERIC keyword on the ADDSD command. Ask your group/security administrator or owner for information on the rules for specifying generic characters.

Notice the difference in the profile name for generic profile. Here we use the name USERID.PROJ.* which means that the generic profile we will create protects all data sets with the first two qualifiers USERID.PROJ. In other words the profile will protect USERID.PROJ.ONE, USERID.PROJ.TWO, USERID.PROJ.THREE, etc. For a discrete profile, the profile name would be USERID.PROJ.ONE.

To create a generic profile, issue the ADDSD command. Type:

ADDSD 'profile name with generic character' UACC(level) AUDIT(type(level))

To create a generic profile without using generic characters, issue the ADDSD command. Type:

ADDSD 'profile name' UACC(level) AUDIT(type(level)) GENERIC

The UACC can be only one of the following:

NONE
no access to the data set

READ
read only access to the data set

UPDATE
read and write access to the data set

CONTROL
VSAM control password access to VSAM data set

ALTER
full control of the resource profile for the data set

default =
the value specified in the UACC field in your current connect group.

CAUTION

Anyone who has READ authority (or UPDATE, CONTROL, or ALTER) to your protected user data set can create a copy of it. As owner of the copied data set, that user has control of the security level of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. See Task 10 for information on how to permit selected users or groups to access a data set.

The audit type which specifies the access attempts you want recorded, can be only one of the following and must be entered:

ALL
records all attempts to access the data set

FAILURES
records all unauthorized attempts to access the data set

SUCCESS
records all authorized attempts to access the data set

NONE
no recording

default =
FAILURES

An optional parameter, the audit access level is the access level at which someone attempted to access a protected resource. It can be:

READ
records attempts at any level

UPDATE
records attempts to update a data set

CONTROL
records attempts to update a VSAM data set

ALTER
records attempts to alter the data set

default =
READ

For Example:

To create a generic profile for all user data sets beginning with USERID.PROJ.*, type:

ADDSD 'USERID.PROJ.*' UACC(READ) AUDIT(ALL(READ))

To create a generic profile to protect all data sets that have your userid as the high-level qualifier, type:

ADDSD 'USERID.*' UACC(READ) AUDIT(ALL(READ))

To create a generic profile for all group data sets beginning with GROUPID.PROJ.*, type:

ADDSD 'GROUPID.PROJ.*' UACC(READ) AUDIT(ALL(READ))

To create a generic profile to protect all data sets that have a groupid as the high-level qualifier, type:

ADDSD 'GROUPID.*' UACC(READ) AUDIT(ALL(READ))

If the command fails, you will get a message stating you are not authorized. See your group/security administrator or owner.

If, after a generic profile exists, you want to create a data set that has more specific access requirements than allowed under the existing generic profile, create a discrete profile (or a more specific generic profile) for the data set.

CAUTION

If your installation is an "always-call" installation (that is, RACF is always called each time an attempt is made to access a data set or general resource), keep in mind the that a generic profile might already exist under which the data set might be protected. But the profile might not possess the exact access control information you want for your data set. In this case, you can create a more specific generic profile or a discrete profile for the data set.

To find out if you are in an always call environment, ask your group/security administrator or owner.

Task 10. Permitting An Individual or a Group to Use A Data Set

SITUATION: You would like J.E. Jones to use your RACF protected data set.

You are automatically given ALTER authority for any data set profile you create. Therefore, you have the necessary authority to issue the PERMIT command to permit someone access to your data set. Proceed with STEP 2.

SITUATION: Your department has a RACF-protected group data set that a colleague needs in his/her work. You wish to allow the person to use this group data set.

To permit an individual or a group to use a group data set requires the PERMIT command. Use of this command requires certain authority. As an end user,in most probability , the only condition that you may meet is that you are the owner of the profile or have ALTER authority to the profile. If you know you are the owner or that you have ALTER authority, proceed with STEP 2.

STEP 1. Determining the profile owner and who is on the access list with ALTER authority

To find out the owner and who is on the access list and with what authority, issue the LISTDSD command. Type:

LISTDSD DATASET('profile name ') ALL

Check the OWNER field in the profile listing. If you or your connect group is the owner or if you or your connect group is on the access list with ALTER authority, proceed with STEP 2. If not, log on to the group you need. See Task 14 for information on how to do this. If you need more information on the data set profile, see Task 5.

For example, to check the data set, USERID.PROJ.ONE, type:

LISTDSD DATASET('USERID.PROJ.ONE') ALL

If the command fails, you will get a message stating you are not authorized. See your group/security administrator or owner.

STEP 2. Allowing access to a data set

To allow access to your data set, use the PERMIT command with the ACCESS keyword. Type:

PERMIT 'profile name ' ID(userid or groupid) ACCESS(level)

The access authority level must be one of the following:

NONE
no access to the data set

READ
read only access to the data set

UPDATE
read and write access to the data set

CONTROL
VSAM control password access to VSAM data set

ALTER
full control of the resource profile for the data set

If the command fails, you will get a message stating you are not authorized. Contact the owner to issue the PERMIT command.

CAUTION

Anyone who has READ authority (or UPDATE, CONTROL, or ALTER) to your protected user data set can create a copy of it. As owner of the copied data set, that user has control of the security level of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known.

For Example:

To permit user Jones to read the user data set, SMITH.PROJ.ONE, type:

PERMIT 'SMITH.PROJ.ONE' ID(JONES) ACCESS(READ)

To permit users Jones and Moore to read the user data set, SMITH.PROJ.ONE, type:

PERMIT 'SMITH.PROJ.ONE' ID(JONES, MOORE) ACCESS(READ)

To permit group DEPTD60 to read the user data set, SMITH.PROJ.ONE, type:

PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60) ACCESS(READ)

To permit groups DEPTD60 and DEPTD58 to read the user data set, SMITH.PROJ.ONE, type:

PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60, DEPTD58) ACCESS(READ)

To permit the user, Smith to read group data set, GROUPID.PROJ.ONE, type:

PERMIT 'GROUPID.PROJ.ONE' ID(SMITH) ACCESS(READ)

To permit the users, Smith and Jones to read group data set, GROUPID.PROJ.ONE, type:

PERMIT 'GROUPID.PROJ.ONE' ID(SMITH,JONES) ACCESS(READ)

To permit the group DEPTD60 to read group data set, GROUPID.PROJ.ONE, type:

PERMIT 'GROUPID.PROJ.ONE' ID(DEPTD60) ACCESS(READ)

To permit the groups, DEPTD60 and DEPTD58 to read group data set, GROUPID.PROJ.ONE, type:

PERMIT 'GROUPID.PROJ.ONE' ID(DEPTD60, DEPTD58) ACCESS(READ)

Conditions for using PERMIT command: RACF requires one of the following conditions be met:

- You have the SPECIAL user attribute (see Task 2).
- You have the SPECIAL connect attribute (see Task 2) and the data set is within the scope of the group in which you have the SPECIAL connect attribute.
- You own the data set.
- If a data set is protected by a discrete profile, you are on the access list with ALTER authority, (see STEP 1).
- If a data set is protected by a discrete profile, your current connect group is on the access list with ALTER authority (see STEP 1).
- The UACC is ALTER (see STEP 1).

Task 11. Denying An Individual or a Group Use of A Data Set

SITUATION: You have a particular data set that a colleague who has left the department may still use. For security reasons you wish to exclude the person from using the data set.

You are automatically given ALTER authority for any data set profile you create. Therefore, you have the necessary authority to issue the PERMIT command to deny someone access your own user data set. Proceed with STEP 2.

SITUATION: Your department has a RACF-protected group data set that a colleague who has left the department may still use. You wish to be certain the person can not use this group data set.

To deny an individual or a group use of a group data set requires the PERMIT command. Use of this command requires certain authority. As an end user, the only conditions that you may meet is that you are the owner of the profile or have ALTER authority to the profile. If you know you are the owner or that you have ALTER authority, proceed with STEP 2.

STEP 1. Determining the profile owner and who is on the access list with ALTER authority

To find out the owner and who is on the access list and with what authority, issue the LISTDSD command. Type:

LISTDSD DATASET('profile name') ALL

Check the **OWNER** field and the **USER** and **ACCESS** fields in the profile listing. If you or your connect group is the owner or if you or your connect group is on the access list with ALTER authority, proceed with STEP 2. If you or your connect group is not the owner or if you or your connect group is not on the access list with ALTER authority, you cannot change the access to the data set. If you need more information on the data set profile, see Task 5.

To check the data set, **USERID.PROJ.ONE**, type:

LISTDSD DATASET('USERID.PROJ.ONE') ALL

If the command fails, you will get a message stating you are not authorized. See your group/security administrator or owner.

STEP 2. Denying access to a data set

You may deny access to a data set in two ways. One way is to remove the individual from the access list. This will deny access only if the UACC is NONE. For example, if you delete an individual or group from the access list but the UACC is READ, the individual or group will be able to read the data set.

The second way to deny access is to include the individual or group on the access list but assign the individual or group an access of NONE. To assign an access of NONE is the best procedure to ensure the individual or group will not be able to access the data set.

To deny access by removing a user or a group from the access list, issue the PERMIT command with DELETE keyword. Type:

PERMIT 'profile name ' ID(userid or groupid) DELETE

For Example:

To deny user Jones use of the user data set, SMITH.PROJ.ONE, type:

PERMIT 'SMITH.PROJ.ONE' ID(JONES) DELETE

To deny users, Jones and Moore use of the user data set, SMITH.PROJ.ONE, type:

PERMIT 'SMITH.PROJ.ONE' ID(JONES, MOORE) DELETE

To deny group DEPTD60 use of the user data set, SMITH.PROJ.ONE, type:

PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60) DELETE

To deny groups, DEPTD60 and DEPTD58 use of the user data set, SMITH.PROJ.ONE, type:

PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60, DEPTD58) DELETE

To deny access by assigning a user or group an access of NONE, issue the PERMIT command with the ACCESS keyword.

Type:

PERMIT 'profile name ' ID(userid or groupid) ACCESS(NONE)

For Example:

To deny user Jones use of the user data set, SMITH.PROJ.ONE, type:

PERMIT 'SMITH.PROJ.ONE' ID(JONES) ACCESS(NONE)

To deny users, Jones and Moore the use of the user data set, SMITH.PROJ.ONE, type:

PERMIT 'SMITH.PROJ.ONE' ID(JONES, MOORE) ACCESS(NONE)

To deny group DEPTD60 use of the user data set, SMITH.PROJ.ONE, type:

PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60) ACCESS(NONE)

To deny groups, DEPTD60 and DEPTD58 use of the user data set, SMITH.PROJ.ONE, type:

PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60, DEPTD58) ACCESS(NONE)

If the command fails, you will get a message stating you are not authorized. Contact the owner to issue the PERMIT command.

Conditions for using PERMIT command: RACF requires one of the following conditions be met:

- You have the SPECIAL user attribute (see Task 2).
- You have the SPECIAL connect attribute (see Task 2) and the data set is within the scope of the group in which you have the SPECIAL connect attribute.
- You own the data set.
- If a data set is protected by a discrete profile, you are on the access list with ALTER authority, (see STEP 1).
- If a data set is protected by a discrete profile, your current connect group is on the access list with ALTER authority (see STEP 1).
- The UACC is ALTER (see STEP 1).

Task 12. Protecting a Tape Data Set

SITUATION: You wish to protect a data set which is on tape. To protect a tape data set on a standard-labeled volume, you must protect the volume on which it is placed. (Any data set you then place on that volume is protected under the profile you create for the volume.)

Note that each data set on a volume shares a common access list. Therefore, if you want to protect a data set that has different access requirements, you must place the data set on a different volume and create a different profile for the data set.

STEP 1. Determining if you have the TAPEVOL class authority

To protect a volume, you need CLAUTH (class authority) in the resource class called TAPEVOL. To see if you have TAPEVOL class authority, use the LISTUSER command. Type:

LISTUSER

Check the CLASS-AUTHORIZATIONS field in the profile listing to see if it contains TAPEVOL class authority. If you know the class authorization is TAPEVOL, proceed with STEP 2.

STEP 2. Protecting a tape data set

To protect a tape data set, issue the RDEFINE command. Type:

RDEFINE TAPEVOL('volume name') UACC(level)

The UACC can be only one of the following:

NONE
no access to the data set

READ
read only access to the data set

UPDATE
read and write access to the data set

CONTROL
VSAM control password access to VSAM data set

ALTER
full control of the resource profile for the data set

default =
the value specified in the UACC field in your current connect group. See Task 1 for more information.)

For example, to protect the tape volume, **T11011**, type:

RDEFINE TAPEVOL('T11011') UACC(READ)

If the command fails, you will get a message stating you are not authorized. See your group/security administrator or owner.

Note: For non-standard labeled tape volumes, you can issue the RDEFINE command the same way as for standard-labeled tapes. However, the only protection you will have is through a mount message that will be issued to the operator when an unauthorized user tries to access the volume.

Note: As an alternative to using the RDEFINE command to protect a tape volume, you can use the PROTECT=YES keyword on the JCL statement you use to define the tape data set.

Task 13. Removing Protection From Your Data Set

SITUATION: You have a data set containing experimental data which has been published. You no longer feel it is necessary to protect the data.

If you are the owner of a data set or have ALTER authority, you can remove RACF protection from the data set by deleting the data set profile. If you know you are the owner or that you have ALTER authority, proceed with STEP 2.

STEP 1. Determining the profile owner or if you have the ALTER authority

To find out the profile owner or if you have ALTER authority, issue the LISTDSD command. Type:

LISTDSD DATASET('profile name') ALL

If the command succeeds, you will see profile listing. Check the **OWNER** and the field, **YOUR ACCESS** in the profile listing. If you are the owner or you have ALTER authority, proceed with STEP 2. If the YOUR ACCESS field does not contain ALTER and you are not the owner, see your group/security administrator or owner. If you need more information on how the data set is protected, see Task 5.

If the command fails, you will get a message stating you are not authorized. See your group/security administrator or owner.

For example, to check the data set, **SMITH.PROJ.ONE**, type:

LISTDSD DATASET('SMITH.PROJ.ONE') ALL

STEP 2. Deleting RACF protection

To delete the data set profile, issue the DELDSD command. Type:

DELDSD 'profile name'

This deletes the profile, which removes RACF protection, but leaves the data set intact.

For Example:

To remove RACF protection from the data set, SMITH.PROJ.ONE, type:

DELDSD 'SMITH.PROJ.ONE'

To remove RACF protection from the data sets, SMITH.PROJ.ONE, SMITH.PROJ.TWO, SMITH.PROJ.THREE which are protected by the generic profile, SMITH.PROJ.*, type:

DELDSD 'SMITH.PROJ.*'

Be careful when you delete a generic profile that you are not inadvertently removing RACF protection from a data set that should remain protected. In the above example RACF protection would be removed from any data set whose name matched the profile name, such as SMITH.PROJ.MASTER.

CAUTION

When you delete a data set profile, anyone (RACF-defined or not) can access, change, and/or delete your data set. You can selectively "remove" protection by using the PERMIT command to permit or deny access to your data set by selected users and groups. See Tasks 10 and 11 for detail.

Task 14. Logging On to a Group Other Than Your Default Group

SITUATION: A particular group may use a data set containing a report that is critical to a presentation you are preparing. You need the information.

STEP 1. Determining what groups you belong to

You must first be belong to a group before you can log on to it. If you know that you belong to the group you need, proceed with STEP 2. If you do not know whether you belong to the group you need, use the LISTUSER command, as described in Task 2, to see a list of the groups you belong to.

STEP 2. Logging on to a group other than your default group

For TSO/E Users: This example shows an example of an actual screen. Enter the group name you want to logon to in the group-ident position of the TSO logon screen. The following screen shows a user logging on to group, DEPTD60.

```
ENTER LOGON PARAMETERS BELOW:     RACF LOGON PARAMETERS:

USERID        ======> XYZ1JES

PASSWORD      ======>             NEW PASSWORD ====>

PROCEDURE     ======> PROC01      GROUP IDENT  ====> DEPTD60

ACCT NMBR     ======> A4446B


SIZE          ======>

PERFORM       ======>

COMMAND       ======>
```

For Non-TSO/E Users: Enter:

LOGON userid GROUP(groupname)

The userid is your userid and the groupname is the name of the group you wish to log on to.

For example, to log on to group DEPTD60, type:

LOGON XYZ1JES GROUP(DEPTD60)

PROTECTING YOUR INFORMATION USING RACF ISPF PANELS

Tasks 15 through 22 tell you how to protect your information using RACF ISPF panels. If you are an infrequent user of RACF, you may want to review Task 1 to get you started.

In each task there is a short description of a situation which sets the stage as an example of why you might want to perform the task.

RACF ISPF panels have a tutorial that gives you a general description of RACF. If you would like to view the tutorial, select the RACF option on the ISPF menu. On the next screen you see, select the tutorial option.

Task 15. Finding Out What Authority You Have

SITUATION: You must protect a sensitive data set using RACF but you are not aware of what you can do using RACF.

Select the RACF option on the ISPF menu and RACF will display the following screen.

```
                        RACF SERVICES OPTION MENU

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                      for a DASD data set.

2 GENERAL RESOURCE    ADD, CHANGE, DELETE, or DISPLAY the
                      profile for a general resource.

3 GROUP               ADD, CHANGE, DELETE, or DISPLAY a group
                      profile.
                      CONNECT or REMOVE users.

4 USER                ADD, CHANGE, DELETE, or DISPLAY a
                      user profile.
                      Change a user's password.

5 SYSTEM OPTIONS      DISPLAY or SET the system wide
                      security options.
                      REFRESH in-storage profile lists.

T TUTORIAL            View a general description of RACF.
```

On the OPTION Line, enter 4. Press ENTER.

Option 4 gives you the following screen:

```
                          RACF - USER SERVICES

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 ADD       Add a user profile      D DISPLAY  Display profile
                                               contents

2 CHANGE    Change a user profile   S SEARCH   Search RACF data
                                               set for profiles

3 DELETE    Delete a user profile

4 PASSWORD  Change your own password

5 AUDIT     Monitor users activity

ENTER USER INFORMATION:

USER ID   ===>
```

On the OPTION Line, enter D. Press ENTER.

Option D gives you a listing of your profile. You will see a screen similar to the one shown that displays the contents of your profile.

This portion of the screen describes you as the user.

```
USER=your    NAME=your     OWNER=your    CREATED=date you
     userid       name           owner           were
                                                 defined
                                                 to RACF


DEFAULT-GROUP=your    PASSDATE=date  PASS-INTERVAL=length of
           default     your password         time your password
         group name    was last updated         is valid


ATTRIBUTES=your operating privileges and restrictions


LAST-ACCESS=last date you were on the system


CLASS-AUTHORIZATIONS=installation assigned classes in which
                     the user can define profiles.

INSTALLATION-DATA=information your installation maintains
                  about you


MODEL-NAME=a profile used as a model for new data set
profiles
```

This portion of the screen describes group(s) you belong to and what you can do as a member of the group(s).

```
GROUP=name AUTH=your CONNECT-OWNER=your CONNECT-DATE=date
      of        group                 group        you were
      group     authority             owner        connected
                                                   to group


CONNECTS=number   UACC=universal    LAST-CONNECT=last time
       of times         access                   you were
       you were       authority                  connected
      connected
       to group

CONNECT ATTRIBUTES=your operating privileges
                    as a member of the group
```

For a detailed descriptions of the fields appearing on the screen, see Task 1.

Your owner/administrator creates and maintains your user profile, which describes you to the RACF system. Your profile contains: your owner's name, your userid, information about your operating privileges and restrictions, information about your default group and other groups to which you belong, and other important information. If, after determining what your operating privileges and restrictions are, you need to change your user profile, see your group/ security administrator or owner. **This example shows an actual screen describing a RACF user connected to only one group.**

```
USER=SMITH   NAME=J.E.SMITH   OWNER=JONES   CREATED=84.096

DEFAULT-GROUP=DEPTD60   PASSDATE=84.103  PASS-INTERVAL= 30

ATTRIBUTES=NONE

LAST-ACCESS=84.114/13:47:18

CLASS AUTHORIZATIONS=NONE

NO-INSTALLATION-DATA

NO-MODEL-NAME

GROUP=DEPTD60  AUTH=USE  CONNECT-OWNER=JONES CONNECT-DATE=84.096

 CONNECTS= 05   UACC=NONE   LAST-CONNECT=84.114/13:47:18

   CONNECT ATTRIBUTES=NONE
```

In this example, user, J.E. Smith has none of the possible user attributes. He is still able to use RACF; he can perform such tasks as create data sets and RACF-protect them.

This example shows an actual screen describing a RACF user connected to two groups each with different attributes.

```
USER=SMITH   NAME=J.E.SMITH   OWNER=JONES  CREATED=84.096

DEFAULT-GROUP=SEARCH  PASSDATE=84.103   PASS-INTERVAL= 30

ATTRIBUTES=ADSP

LAST-ACCESS=84.114/13:47:18

CLASS AUTHORIZATIONS=NONE

NO-INSTALLATION-DATA

MODEL-NAME=SMITH.MODEL

GROUP=SEARCH AUTH=JOIN CONNECT-OWNER=WILL CONNECT-DATE=84.096

   CONNECTS= 01   UACC=NONE   LAST-CONNECT=84.114/13:50:18

   CONNECT ATTRIBUTES=NONE

GROUP=PAYROLL AUTH=CREATE CONNECT-OWNER=MILL CONNECT-DATE=84.096

   CONNECTS= 00  UACC=READ  LAST-CONNECT=84.114/13:55:18

   CONNECT ATTRIBUTES=NONE
```

In this example, user, J.E. Smith has the user attribute, ADSP. A user attribute overrides any connect (group-level) attribute. If you have a more powerful attribute as a user it takes precedent over a lesser connect (group-level) attribute. What you can do as a user you can do as a member of a group. With the ADSP attribute, RACF automatically protects all of Smith's permanent data sets. Smith also has a model data set profile so whenever Smith creates a permanent data set, RACF uses the name of the data set appearing in the MODEL-NAME as a model for the new data set profile.

Smith also belongs to two different groups, SEARCH and PAYROLL. In the SEARCH group, Smith can assign group authorities to members of the group. In the PAYROLL group, Smith can RACF-protect a data set and decide who can use the data set.

Smith also has the UACC = READ. UACC stands for universal access authority which means that any user not specifically mentioned in the access list describing a resource, may use the resource in the manner specified in the UACC. In this case, when Smith defines a PAYROLL data set the UACC is set to READ unless Smith sets the the UACC to another value. All RACF-defined users have read only access to the data set.

If Smith belonged to any other groups, the screen would also list the information about those groups.

If you find that you are unable to perform a certain task adequately because you are not connected to the necessary group(s) or your authority is not sufficient contact your group/security administrator or owner.

Task 16. Finding Out What Profiles You Have

SITUATION: You created a data set that needs protection but you do not know whether you currently have a profile that will protect the data set.

Select the RACF option on the ISPF menu and RACF will display the following screen.

```
                          RACF SERVICES OPTION MENU

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 DATA SET              ADD, CHANGE, DELETE, or DISPLAY the profile
                        for a DASD data set.

2 GENERAL RESOURCE      ADD, CHANGE, DELETE, or DISPLAY the
                        profile for a general resource.

3 GROUP                 ADD, CHANGE, DELETE, or DISPLAY a group
                        profile.
                        CONNECT or REMOVE users.

4 USER                  ADD, CHANGE, DELETE, or DISPLAY a
                        user profile.
                        Change a user's password.

5 SYSTEM OPTIONS        DISPLAY or SET the system wide
                        security options.
                        REFRESH in-storage profile lists.

T TUTORIAL              View a general description of RACF.
```

On the OPTION Line, enter 1. Press ENTER.

Option 1 gives you the following screen:

```
                        RACF - DATA SET SERVICES

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 ADD          Add a profile        D DISPLAY    Display profile
                                                 contents

2 CHANGE       Change a profile     S SEARCH     Search RACF data
                                                 set for profiles

3 DELETE       Delete a profile

4 ACCESS       Maintain access list

5 AUDIT        Monitor access attempts
                (for auditors only)

ENTER DATA SET PROFILE INFORMATION:

PROFILE NAME        ===>

GENERIC             ===>   YES If the profile name is generic

VOLUME SERIAL       ===>   If the data set is not cataloged

UNIT                ===>   If option 1 and VOLUME SERIAL entered

DATA SET PASSWORD   ===>   If the data set is password protected
```

On the OPTION Line, enter S. Press ENTER.

Option S gives you the following screen:

```
                    RACF - SEARCH FOR DATA SET PROFILES

COMMAND ===>

ENTER OPTIONAL SELECTION CRITERIA:

MASK1 ===>
                    MASK1 selects profile names starting with
                    the specified character string.
MASK2 ===>
                    MASK2 selects profile names containing the
                    specified string somewhere after the MASK1 string.

AGE   ===>          Selects profiles that have not been accessed
                    within the number of days specified.

TYPE  ===>          GENERIC, DISCRETE, VSAM, NONVSAM,
                    MODEL, WARNING, or ALL

VOLUMES ===>     ===>        ===>        ===>        ===>
        ===>     ===>        ===>        ===>        ===>

CLIST   ===>     To generate a TSO CLIST, enter YES
```

Enter the requested information in the fields on the screen. Press ENTER.

MASK1 is the high-level qualifier while MASK 2 is the second-level qualifier in the profile name.

RACF will list all your profiles. If you do not have any profiles, RACF will display a message telling there are no profiles.

For Example:

To find out what profiles you have with your userid as the high-level qualifier, complete the screen as shown:

```
                    RACF - SEARCH FOR DATA SET PROFILES

COMMAND ===>

ENTER OPTIONAL SELECTION CRITERIA:

MASK1 ===> YOUR USERID
                 MASK1 selects profile names starting with
                 the specified character string.
MASK2 ===>
                 MASK2 selects profile names containing the
                 specified string somewhere after the MASK1 string.

AGE   ===>       Selects profiles that have not been accessed
                 within the number of days specified.

TYPE  ===> ALL   GENERIC, DISCRETE, VSAM, NONVSAM,
                 MODEL, WARNING, or ALL

VOLUMES ===>     ===>       ===>       ===>       ===>
        ===>     ===>       ===>       ===>       ===>

CLIST   ===>     To generate a TSO CLIST, enter YES
```

RACF would list all the profiles with your userid as the high-level qualifier.

Task 17. Changing Your Password

SITUATION: You suspect that your password has become known to others. Or, perhaps you would prefer to change your password more frequently than your installation requires.

In choosing a new password, be aware that your installation has password rules. If you do not know the rules, choose a password following the format of your current password. RACF may also not allow you to re-use a previous password. See your group/security administrator or owner for an explanation of your installation's rules for passwords.

Select the RACF option on the ISPF menu and RACF will display the following screen.

```
                          RACF SERVICES OPTION MENU

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                      for a DASD data set.

2 GENERAL RESOURCE    ADD, CHANGE, DELETE, or DISPLAY the
                      profile for a general resource.

3 GROUP               ADD, CHANGE, DELETE, or DISPLAY a group
                      profile.
                      CONNECT or REMOVE users.

4 USER                ADD, CHANGE, DELETE, or DISPLAY a
                      user profile.
                      Change a user's password.

5 SYSTEM OPTIONS      DISPLAY or SET the system wide
                      security options.
                      REFRESH in-storage profile lists.

T TUTORIAL            View a general description of RACF.
```

On the OPTION Line, enter 4. Press ENTER.

Option 4 gives you the following screen:

```
                              RACF - USER SERVICES

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 ADD        Add a user profile      D DISPLAY  Display profile
                                                 contents

2 CHANGE     Change a user profile   S SEARCH   Search RACF data
                                                 set for profiles

3 DELETE     Delete a user profile

4 PASSWORD   Change your own password

5 AUDIT      Monitor users activity

ENTER USER INFORMATION:

USER ID    ===>
```

On the OPTION Line, enter 4. Press ENTER.

Option 4 gives you the following screen:

```
                    RACF - CHANGE USER PASSWORD  - USERID

COMMAND ===>

ENTER THE FOLLOWING:

   CURRENT PASSWORD  ===>

   NEW PASSWORD      ===>
```

To change your password, enter the requested information. Press ENTER.

If you have chosen an incorrect password, you will get a message stating that the password has not been changed. See your group/security administrator or owner for an explanation of your installation's rules for passwords.

You may also change your password during logon, see Task 1.

For Example:

To change your password from "subject" to "tester" complete the screen as follows:

```
                RACF - CHANGE USER PASSWORD  - USERID

COMMAND ===>

ENTER THE FOLLOWING:

   CURRENT PASSWORD  ===>  subject

   NEW PASSWORD      ===>  tester
```

Task 18. Finding Out How a Data Set is Protected

SITUATION: Suppose you want to restrict a data set to only a few people, but you are not aware of the current status of the data set.

Select the RACF option on the ISPF menu and RACF will display the following screen.

```
                        RACF SERVICES OPTION MENU

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 DATA SET              ADD, CHANGE, DELETE, or DISPLAY the profile
                        for a DASD data set.

2 GENERAL RESOURCE      ADD, CHANGE, DELETE, or DISPLAY the
                        profile for a general resource.

3 GROUP                 ADD, CHANGE, DELETE, or DISPLAY a group
                        profile.
                        CONNECT or REMOVE users.

4 USER                  ADD, CHANGE, DELETE, or DISPLAY a
                        user profile.
                        Change a user's password.

5 SYSTEM OPTIONS        DISPLAY or SET the system wide
                        security options.
                        REFRESH in-storage profile lists.

T TUTORIAL              View a general description of RACF.
```

On the OPTION Line, enter 1. Press ENTER.

Option 1 gives you the following screen:

```
                        RACF - DATA SET SERVICES

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 ADD          Add a profile        D DISPLAY    Display profile
                                                 contents

2 CHANGE       Change a profile     S SEARCH     Search RACF data
                                                 set for profiles

3 DELETE       Delete a profile

4 ACCESS       Maintain access list

5 AUDIT        Monitor access attempts
                (for auditors only)

ENTER DATA SET PROFILE INFORMATION:

PROFILE NAME       ===>

GENERIC            ===>   YES If the profile name is generic

VOLUME SERIAL      ===>   If the data set is not cataloged

UNIT               ===>   If option 1 and VOLUME SERIAL entered

DATA SET PASSWORD  ===>   If the data set is password protected
```

On the OPTION line, enter D. Enter the profile name and any other appropriate information. Press ENTER.

For a discrete profile, the profile name and data set name are the same.

Option D gives you the following screen:

```
                                RACF - DISPLAY DATA SET PROFILE

COMMAND ===>

PROFILE NAME: <<<profile name>>>

TO SELECT INFORMATION TO BE DISPLAYED, ENTER YES:

ACCESS LIST ===>          Profile access list

HISTORY     ===>          Profile history

STATISTICS  ===>          Profile use statistics

TO LIMIT THE DISPLAY TO PROFILES FOR DATA SETS ON
SPECIFIC VOLUMES,

ENTER VOLUME SERIAL NUMBER(s):

===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
```

Enter YES in the categories that you want information displayed about the profile.

If you get a message stating you are not authorized, see your group/security administrator or owner.

The information you see is the listing of the profile. It will be similar to the following example:

```
 LEVEL        OWNER          UNIVERSAL ACCESS     WARNING
 -----        -----          ----------------     -------
  00          SMITH               READ              NO

  AUDITING
 ----------
  SUCCESS (UPDATE)

  YOUR ACCESS          CREATION GROUP          DATASET TYPE
--------------       ---------------       -------------
   READ                   DEPTD60               NON-VSAM

 VOLUMES ON WHICH DATASET RESIDES              UNIT
----------------------------------            ------
           21345                              SYSDA

INSTALLATION DATA
------------------
PL/1 LINK LIBRARY

CREATION DATE      LAST REFERENCE DATE      LAST CHANGE DATE
(DAY)  (YEAR)       (DAY)      (YEAR)        (DAY)   (YEAR)
-------------      ------------------      ---------------
 070    85           070        85            070     85

ALTER COUNT     CONTROL COUNT     UPDATE COUNT     READ COUNT
-----------     -------------     ------------     ----------
 00000            00000             00002           00000

USER           ACCESS                ACCESS COUNT
----          --------               --------------
JONES          UPDATE                  00009
WILLS          READ                    00015
  *              *                       *
  *              *                       *
```

Check the following fields for the most important security information about how the data set is protected:

- the OWNER field
- the UACC field
- the USER field
- the ACCESS field

Here are brief descriptions of the terms appearing on the screen:

LEVEL
An indicator used by each individual installation. If anything other than 00 appears in this field, see your group/security administrator or owner for an explanation of what the number means.

OWNER
Each RACF-defined data set has an owner. An owner may be an individual or a group. When you create a data set and then RACF-protect the data set without specifying an owner, RACF names you the owner of the data set profile. The owner of the profile may modify the data set profile.

UNIVERSAL ACCESS
Each data set protected by RACF has a universal access authority (UACC). The UACC permits individuals or groups to use the data set in the manner specified in this field. In this example, the UACC is READ. Anyone may read this data set. (The only exception is if the individual is specifically named in the access list with a UACC of NONE.)

WARNING
If this field contains YES, RACF permits a user to access this resource even though his/her access authority is insufficient and will issue a warning message describing this condition. If this field contains NO, RACF does not permit a user with insufficient authority to access this resource.

AUDITING
The type of access attempts that are recorded. In this example, the AUDITING is SUCCESS (UPDATE). RACF will record all successfully attempts to update the data set.

YOUR ACCESS
How you may access this data set. If NONE appears in this field, you cannot access the data set.

CREATION GROUP
The group under which the profile was created.

DATASET TYPE
The data set type. It may be either VSAM or non-VSAM.

VOLUME ON WHICH THE DATASET RESIDES
The volume on which a non-VSAM data set resides or the volume on which the catalog for a VSAM data set resides.

UNIT
The unit type on for a non-VSAM data set

INSTALLATION DATA
Any information your installation keeps in this data set profile.

CREATION DATE
The date the profile was created.

LAST REFERENCE DATE
The last time the profile was accessed.

LAST CHANGE DATE
The last time the profile was changed.

ALTER COUNT
The number of times the profile was altered.

CONTROL COUNT
The number of times the profile was successfully accessed with CONTROL authority.

UPDATE COUNT
The number of times the profile was successfully accessed with UPDATE authority.

READ COUNT
The number of times the profile was successfully accessed with READ authority.

USER
Any specific users or groups permitted access to the data set.

ACCESS
How any users listed in the USER field accessed the data.

ACCESS COUNT
The number of times any users listed in the USER field accessed the data set.

Task 19. Changing A Data Set's Access Authority (UACC)

SITUATION: You have a data set containing research data. There is a need to protect the information so that no one can tamper with the experimental data.

Select the RACF option on the ISPF menu and RACF will display the following screen.

```
                        RACF SERVICES OPTION MENU

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                      for a DASD data set.

2 GENERAL RESOURCE    ADD, CHANGE, DELETE, or DISPLAY the
                      profile for a general resource.

3 GROUP               ADD, CHANGE, DELETE, or DISPLAY a group
                      profile.
                      CONNECT or REMOVE users.

4 USER                ADD, CHANGE, DELETE, or DISPLAY a
                      user profile.
                      Change a user's password.

5 SYSTEM OPTIONS      DISPLAY or SET the system wide
                      security options.
                      REFRESH in-storage profile lists.

T TUTORIAL            View a general description of RACF.
```

On the OPTION Line, enter 1. Press ENTER.

Option 1 gives you the following screen:

```
                        RACF - DATA SET SERVICES

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 ADD          Add a profile        D DISPLAY    Display profile
                                                 contents

2 CHANGE       Change a profile     S SEARCH     Search RACF data
                                                 set for profiles

3 DELETE       Delete a profile

4 ACCESS       Maintain access list

5 AUDIT        Monitor access attempts
                (for auditors only)

ENTER DATA SET PROFILE INFORMATION:

PROFILE NAME       ===>

GENERIC            ===>   YES If the profile name is generic

VOLUME SERIAL      ===>   If the data set is not cataloged

UNIT               ===>   If option 1 and VOLUME SERIAL entered

DATA SET PASSWORD  ===>   If the data set is password protected
```

On the OPTION line, enter 2. Enter the profile name and any other appropriate information. Press ENTER.

For a discrete profile, the profile name and data set name are the same.

Option 2 gives you the following screen:

```
                    RACF - CHANGE DATA SET PROFILE

COMMAND ===>

PROFILE NAME: <<<profile name>>>

ENTER DATA SET PROFILE INFORMATION TO BE CHANGED:

OWNER              ===>        Userid or group name

LEVEL              ===>        0-99

FAILED ACCESSES    ===>        FAIL or WARN

UACC               ===>        NONE, READ, UPDATE, CONTROL,
                               or ALTER

AUDIT SUCCESSES    ===>        READ, UPDATE, CONTROL, ALTER,
                               or NOAUDIT

AUDIT FAILURES     ===>        READ, UPDATE, CONTROL, ALTER,
                               or NOAUDIT

TO DISPLAY THE PANELS FOR CHANGING OPTIONAL INFORMATION,
ENTER YES:

VOLUMES            ===>

INSTALLATION DATA  ===>

ACCESS LIST        ===>
```

Enter the UACC you want to assign to this profile.

The UACC values are:

NONE
no access to the data set

READ
read only access to the data set

UPDATE
read and write access to the data set

CONTROL
VSAM control password access to VSAM data set

ALTER
full control of the resource profile for the data set

If you get a message stating you are not authorized, see your group/security administrator or owner.

CAUTION

Anyone who has READ authority (or UPDATE, CONTROL, or ALTER) to your protected user data set can create a copy of it. As owner of the copied data set, that user has control of the security level of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See Task 23 for information on how to permit selected users or groups to access a data set.

For Example:

To change the UACC for the profile, USERID.PROJ.ONE to NONE, complete the screen as follows:

```
                    RACF - CHANGE DATA SET PROFILE

COMMAND ===>

PROFILE NAME: <<<USERID.PROJ.ONE>>>

ENTER DATA SET PROFILE INFORMATION TO BE CHANGED:

OWNER              ===>        Userid or group name

LEVEL              ===>        0-99

FAILED ACCESSES    ===>        FAIL or WARN

UACC               ===> NONE   NONE, READ, UPDATE, CONTROL,
                               or ALTER

AUDIT SUCCESSES    ===>        READ, UPDATE, CONTROL, ALTER,
                               or NOAUDIT

AUDIT FAILURES     ===>        READ, UPDATE, CONTROL, ALTER,
                               or NOAUDIT

TO DISPLAY THE PANELS FOR CHANGING OPTIONAL INFORMATION,
ENTER YES:

VOLUMES            ===>

INSTALLATION DATA  ===>

ACCESS LIST        ===>
```

Task 20. Changing A Data Set's Audit Type

SITUATION: You would like tighter control over a particular data set. You want to know all attempts to use the data set.

Select the RACF option on the ISPF menu and RACF will display the following screen.

```
                        RACF SERVICES OPTION MENU

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                      for a DASD data set.

2 GENERAL RESOURCE    ADD, CHANGE, DELETE, or DISPLAY the
                      profile for a general resource.

3 GROUP               ADD, CHANGE, DELETE, or DISPLAY a group
                      profile.
                      CONNECT or REMOVE users.

4 USER                ADD, CHANGE, DELETE, or DISPLAY a
                      user profile.
                      Change a user's password.

5 SYSTEM OPTIONS      DISPLAY or SET the system wide
                      security options.
                      REFRESH in-storage profile lists.

T TUTORIAL            View a general description of RACF.
```

On the OPTION Line, enter 1. Press ENTER.

Option 1 gives you the following screen:

```
                        RACF - DATA SET SERVICES

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 ADD          Add a profile       D DISPLAY    Display profile
                                                contents

2 CHANGE       Change a profile    S SEARCH     Search RACF data
                                                set for profiles

3 DELETE       Delete a profile

4 ACCESS       Maintain access list

5 AUDIT        Monitor access attempts
                (for auditors only)


ENTER DATA SET PROFILE INFORMATION:


PROFILE NAME       ===>

GENERIC            ===>   YES If the profile name is generic

VOLUME SERIAL      ===>   If the data set is not cataloged

UNIT               ===>   If option 1 and VOLUME SERIAL entered

DATA SET PASSWORD ===>    If the data set is password protected
```

On the OPTION line, enter 2. Enter the profile name and any other appropriate information. Press ENTER.

For a discrete profile, the profile name and data set name are the same.

Option 2 gives you the following screen:

```
                    RACF - CHANGE DATA SET PROFILE

COMMAND ===>

PROFILE NAME: <<<profile name>>>

ENTER DATA SET PROFILE INFORMATION TO BE CHANGED:

OWNER              ===>        Userid or group name

LEVEL              ===>        0-99

FAILED ACCESSES    ===>        FAIL or WARN

UACC               ===>        NONE, READ, UPDATE, CONTROL,
                               or ALTER

AUDIT SUCCESSES    ===>        READ, UPDATE, CONTROL, ALTER,
                               or NOAUDIT

AUDIT FAILURES     ===>        READ, UPDATE, CONTROL, ALTER,
                               or NOAUDIT

TO DISPLAY THE PANELS FOR CHANGING OPTIONAL INFORMATION,
ENTER YES:

VOLUMES            ===>

INSTALLATION DATA  ===>

ACCESS LIST        ===>
```

Enter the AUDIT type you want to assign to this profile.

The audit type specifies which access attempts you want recorded, There are two categories:

AUDIT FAILURES
records all unauthorized attempts to access the data set

AUDIT SUCCESSES
records all authorized attempts to access the data set

The values in each category are:

READ
records attempts at any level

UPDATE
records attempts to update a data set

CONTROL
records attempts to update a VSAM data set

ALTER
records attempts to alter the data set

NOAUDIT
no recording

If you get a message stating you are not authorized, see your group/security administrator or owner.

For Example:

To change the audit type for the profile, USERID.PROJ.ONE to record both successful and unsuccessful all access attempts, complete the screen as follows:

```
                    RACF - CHANGE DATA SET PROFILE

COMMAND ===>

PROFILE NAME: <<<USERID.PROJ.ONE>>>

ENTER DATA SET PROFILE INFORMATION TO BE CHANGED:

OWNER              ===>        Userid or group name

LEVEL              ===>        0-99

FAILED ACCESSES    ===>        FAIL or WARN

UACC               ===>        NONE, READ, UPDATE, CONTROL,
                               or ALTER

AUDIT SUCCESSES    ===> READ   READ, UPDATE, CONTROL, ALTER,
                               or NOAUDIT

AUDIT FAILURES     ===> READ   READ, UPDATE, CONTROL, ALTER,
                               or NOAUDIT

TO DISPLAY THE PANELS FOR CHANGING OPTIONAL INFORMATION,
ENTER YES:

VOLUMES            ===>

INSTALLATION DATA  ===>

ACCESS LIST        ===>
```

For Example:

To change the audit type for the profile, GROUPID.PROJ.ONE to record both successful and unsuccessful update access attempts, complete the screen as follows:

```
                    RACF - CHANGE DATA SET PROFILE

COMMAND ===>

PROFILE NAME: <<<GROUPID.PROJ.ONE>>>

ENTER DATA SET PROFILE INFORMATION TO BE CHANGED:

OWNER              ===>           Userid or group name

LEVEL              ===>           0-99

FAILED ACCESSES    ===>           FAIL or WARN

UACC               ===>           NONE, READ, UPDATE, CONTROL,
                                  or ALTER

AUDIT SUCCESSES    ===> UPDATE    READ, UPDATE, CONTROL, ALTER,
                                  or NOAUDIT

AUDIT FAILURES     ===> UPDATE    READ, UPDATE, CONTROL, ALTER,
                                  or NOAUDIT

TO DISPLAY THE PANELS FOR CHANGING OPTIONAL INFORMATION,
ENTER YES:

VOLUMES            ===>

INSTALLATION DATA ===>

ACCESS LIST        ===>
```

Task 21. Creating A Discrete Profile To Protect a Data Set

SITUATION: You have a single data set that need to be protected with very specific requirements or one of your more sensitive user data sets is not currently protected.

In either case, you will create a *discrete profile* for the data set to establish the unique access characteristics you want. When you create a profile, either discrete or generic, you are establishing RACF protection for a data set.

Select the RACF option on the ISPF menu and RACF will display the following screen.

```
                        RACF SERVICES OPTION MENU

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                      for a DASD data set.

2 GENERAL RESOURCE    ADD, CHANGE, DELETE, or DISPLAY the
                      profile for a general resource.

3 GROUP               ADD, CHANGE, DELETE, or DISPLAY a group
                      profile.
                      CONNECT or REMOVE users.

4 USER                ADD, CHANGE, DELETE, or DISPLAY a
                      user profile.
                      Change a user's password.

5 SYSTEM OPTIONS      DISPLAY or SET the system wide
                      security options.
                      REFRESH in-storage profile lists.

T TUTORIAL            View a general description of RACF.
```

On the OPTION Line, enter 1. Press ENTER.

Option 1 gives you the following screen:

```
                        RACF - DATA SET SERVICES

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 ADD          Add a profile        D DISPLAY    Display profile
                                                 contents

2 CHANGE       Change a profile     S SEARCH     Search RACF data
                                                 set for profiles

3 DELETE       Delete a profile

4 ACCESS       Maintain access list

5 AUDIT        Monitor access attempts
                (for auditors only)

ENTER DATA SET PROFILE INFORMATION:


PROFILE NAME       ===>

GENERIC            ===>   YES If the profile name is generic

VOLUME SERIAL      ===>   If the data set is not cataloged

UNIT               ===>   If option 1 and VOLUME SERIAL entered

DATA SET PASSWORD  ===>   If the data set is password protected
```

On the OPTION line, enter 1. Enter the profile name and any other appropriate information. Press ENTER.

Option 1 gives you the following screen:

```
                          RACF - ADD DATA SET PROFILE

COMMAND ===>

    PROFILE NAME: <<<profile name>>>

ENTER OR CHANGE DATA SET PROFILE INFORMATION:

OWNER              ===>       Userid or group name

LEVEL              ===>       0-99

FAILED ACCESSES    ===>       FAIL or WARN

UACC               ===>       NONE, READ, UPDATE, CONTROL,
                              or ALTER

AUDIT SUCCESSES    ===>       READ, UPDATE, CONTROL, ALTER,
                              or NOAUDIT

AUDIT FAILURES     ===>       READ, UPDATE, CONTROL, ALTER,
                              or NOAUDIT

TYPE               ===>       Blank or MODEL

INDICATOR          ===>       SET or NOSET

TO DISPLAY THE PANELS FOR ADDING OPTIONAL INFORMATION,
ENTER YES:

OTHER VOLUMES      ===>

INSTALLATION DATA  ===>

ACCESS LIST        ===>
```

Enter the requested information about the profile you are creating.

CAUTION

Anyone who has READ authority (or UPDATE, CONTROL, or ALTER) to your protected user data set can create a copy of it. As owner of the copied data set, that user has control of the security level of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See Task 23 for information on how to permit selected users or groups to access a data set.

For Example:

To create a discrete profile for your data set, USERID.PROJ.ONE, with a UACC of NONE and no recording of attempts to access the data set, complete the screen as follows:

```
                        RACF - ADD DATA SET PROFILE

COMMAND ===>

    PROFILE NAME: <<<USERID.PROJ.ONE>>>

ENTER OR CHANGE DATA SET PROFILE INFORMATION:

OWNER             ===>          Userid or group name

LEVEL             ===>          0-99

FAILED ACCESSES   ===>          FAIL or WARN

UACC              ===> NONE     NONE, READ, UPDATE, CONTROL,
                                or ALTER

AUDIT SUCCESSES   ===> NOAUDIT  READ, UPDATE, CONTROL, ALTER,
                                or NOAUDIT

AUDIT FAILURES    ===> NOAUDIT  READ, UPDATE, CONTROL, ALTER,
                                or NOAUDIT

TYPE              ===>          Blank or MODEL

INDICATOR         ===>          SET or NOSET

TO DISPLAY THE PANELS FOR ADDING OPTIONAL INFORMATION,
ENTER YES:

OTHER VOLUMES     ===>

INSTALLATION DATA ===>

ACCESS LIST       ===>
```

For Example:

To create a discrete profile for the group data set, GROUPID.PROJ.ONE, with a UACC of READ and recording successful attempts to access the data set, complete the screen as follows:

```
                        RACF - ADD DATA SET PROFILE

COMMAND ===>

    PROFILE NAME: <<<USERID.PROJ.ONE>>>

ENTER OR CHANGE DATA SET PROFILE INFORMATION:

OWNER             ===>          Userid or group name

LEVEL             ===>          0-99

FAILED ACCESSES   ===>          FAIL or WARN

UACC              ===> READ     NONE, READ, UPDATE, CONTROL,
                                or ALTER

AUDIT SUCCESSES   ===> UPDATE   READ, UPDATE, CONTROL, ALTER,
                                or NOAUDIT

AUDIT FAILURES    ===> NOAUDIT  READ, UPDATE, CONTROL, ALTER,
                                or NOAUDIT

TYPE              ===>          Blank or MODEL

INDICATOR         ===>          SET or NOSET

TO DISPLAY THE PANELS FOR ADDING OPTIONAL INFORMATION,
ENTER YES:

OTHER VOLUMES     ===>

INSTALLATION DATA ===>

ACCESS LIST       ===>
```

Task 22. Creating A Generic Profile To Protect Data Sets

SITUATION: You have several data sets that have similar security requirements. For general use you can create a *generic profile* rather than a discrete profile and then selectively permit each user or group to access the data.

For a generic profile, RACF ignores the unit and volume information because the data sets protected under the generic profile might be on many different volumes. Further, when a data set protected by a generic profile is scratched, the profile remains intact (unlike a discrete profile).

To create a generic profile for your user data set, the high level qualifier must be your userid.

To create a generic profile for a group data set, you must have either the SPECIAL attribute at the user or group level or CREATE authority in the group.

You create a generic profile in the same manner as a discrete profile, except that you include one or more generic characters (% or *) in the profile name you specify. (Ask your group/security administrator or owner for information on the rules for specifying generic characters.)

Notice the difference in the profile name for generic profile. Here we use the name USERID.PROJ.* which means that the generic profile we will create protects all data sets with the first two qualifiers USERID.PROJ. In other words the profile will protect USERID.PROJ.ONE, USERID.PROJ.TWO, USERID.PROJ.THREE, etc. For a discrete profile, the profile name would be USERID.PROJ.ONE.

Select the RACF option on the ISPF menu and RACF will display the following screen.

```
                        RACF SERVICES OPTION MENU

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                      for a DASD data set.

2 GENERAL RESOURCE    ADD, CHANGE, DELETE, or DISPLAY the
                      profile for a general resource.

3 GROUP               ADD, CHANGE, DELETE, or DISPLAY a group
                      profile.
                      CONNECT or REMOVE users.

4 USER                ADD, CHANGE, DELETE, or DISPLAY a
                      user profile.
                      Change a user's password.

5 SYSTEM OPTIONS      DISPLAY or SET the system wide
                      security options.
                      REFRESH in-storage profile lists.

T TUTORIAL            View a general description of RACF.
```

On the OPTION Line, enter 1. Press ENTER.

Option 1 gives you the following screen:

```
                        RACF - DATA SET SERVICES

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 ADD          Add a profile       D DISPLAY    Display profile
                                                contents

2 CHANGE       Change a profile    S SEARCH     Search RACF data
                                                set for profiles

3 DELETE       Delete a profile

4 ACCESS       Maintain access list

5 AUDIT        Monitor access attempts
                 (for auditors only)


ENTER DATA SET PROFILE INFORMATION:


PROFILE NAME       ===>

GENERIC            ===>   YES If the profile name is generic

VOLUME SERIAL      ===>   If the data set is not cataloged

UNIT               ===>   If option 1 and VOLUME SERIAL entered

DATA SET PASSWORD ===>    If the data set is password protected
```

On the OPTION line, enter 1. Enter the profile name and any other appropriate information. Press ENTER.

Option 1 gives you the following screen:

```
                              RACF - ADD DATA SET PROFILE

COMMAND ===>

    PROFILE NAME: <<<profile name>>>

ENTER OR CHANGE DATA SET PROFILE INFORMATION:

OWNER              ===>       Userid or group name
LEVEL              ===>       0-99
FAILED ACCESSES    ===>       FAIL or WARN
UACC               ===>       NONE, READ, UPDATE, CONTROL,
                              or ALTER
AUDIT SUCCESSES    ===>       READ, UPDATE, CONTROL, ALTER,
                              or NOAUDIT
AUDIT FAILURES     ===>       READ, UPDATE, CONTROL, ALTER,
                              or NOAUDIT
TYPE               ===>       Blank or MODEL
INDICATOR          ===>       SET or NOSET

TO DISPLAY THE PANELS FOR ADDING OPTIONAL INFORMATION,
ENTER YES:

OTHER VOLUMES      ===>
INSTALLATION DATA  ===>
ACCESS LIST        ===>
```

Enter the requested information about the profile you are creating.

If you get a message stating you are not authorized, see your group/security administrator or owner.

If, after a generic profile exists, you want to create a data set that has more specific access requirements than allowed under the existing generic profile, create a discrete profile (or a more specific generic profile) for the data set.

CAUTION

Anyone who has READ authority (or UPDATE, CONTROL, or ALTER) to your protected user data set can create a copy of it. As owner of the copied data set, that user has control of the security level of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See Task 23 for information on how to permit selected users or groups to access a data set.

For Example:

To create a generic profile, USERID.*, with a UACC of NONE and no recording of attempts to access the data set, complete the screen as follows:

```
                        RACF - ADD DATA SET PROFILE

COMMAND ===>

    PROFILE NAME: <<<USERID.*>>>

ENTER OR CHANGE DATA SET PROFILE INFORMATION:

OWNER             ===>          Userid or group name

LEVEL             ===>          0-99

FAILED ACCESSES   ===>          FAIL or WARN

UACC              ===> NONE     NONE, READ, UPDATE, CONTROL,
                                or ALTER

AUDIT SUCCESSES   ===> NOAUDIT  READ, UPDATE, CONTROL, ALTER,
                                or NOAUDIT

AUDIT FAILURES    ===> NOAUDIT  READ, UPDATE, CONTROL, ALTER,
                                or NOAUDIT

TYPE              ===>          Blank or MODEL

INDICATOR         ===>          SET or NOSET

TO DISPLAY THE PANELS FOR ADDING OPTIONAL INFORMATION,
ENTER YES:

OTHER VOLUMES     ===>

INSTALLATION DATA ===>

ACCESS LIST       ===>
```

Task 23. Permitting An Individual or a Group to Use A Data Set

SITUATION: You would like J.E. Jones to use your RACF protected data set.

SITUATION: You have a group data set that a colleague needs in his/her work. You wish allow the person to use this group data set.

Select the RACF option on the ISPF menu and RACF will display the following screen.

```
                        RACF SERVICES OPTION MENU

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                      for a DASD data set.

2 GENERAL RESOURCE    ADD, CHANGE, DELETE, or DISPLAY the
                      profile for a general resource.

3 GROUP               ADD, CHANGE, DELETE, or DISPLAY a group
                      profile.
                      CONNECT or REMOVE users.

4 USER                ADD, CHANGE, DELETE, or DISPLAY a
                      user profile.
                      Change a user's password.

5 SYSTEM OPTIONS      DISPLAY or SET the system wide
                      security options.
                      REFRESH in-storage profile lists.

T TUTORIAL            View a general description of RACF.
```

On the OPTION Line enter, 1. Press ENTER.

Option 1 gives you the following screen:

```
                        RACF - DATA SET SERVICES

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 ADD          Add a profile        D DISPLAY    Display profile
                                                 contents

2 CHANGE       Change a profile     S SEARCH     Search RACF data
                                                 set for profiles

3 DELETE       Delete a profile

4 ACCESS       Maintain access list

5 AUDIT        Monitor access attempts
                (for auditors only)

ENTER DATA SET PROFILE INFORMATION:

PROFILE NAME       ===>

GENERIC            ===>   YES If the profile name is generic

VOLUME SERIAL      ===>   If the data set is not cataloged

UNIT               ===>   If option 1 and VOLUME SERIAL entered

DATA SET PASSWORD ===>    If the data set is password protected
```

On the OPTION line, enter 4. Enter the profile name and any other appropriate information. Press ENTER.

Option 4 gives you the following screen:

```
                        RACF - MAINTAIN DATA SET ACCESS LIST

OPTION ===>

PROFILE NAME: <<<profile name>>>

SELECT ONE OF THE FOLLOWING:

1 ADD       Add users or groups, and/or
            Copy the access list from an existing profile.

2 REMOVE    Remove specified users or groups from
            the access list.

3 RESET     Remove all users and groups from the
            access list.
```

On the OPTION line, enter 1. Press ENTER.

Option 1 gives you the following screen:

```
                    RACF - MAINTAIN DATA SET ACCESS LIST - ADD

COMMAND ===>

PROFILE NAME: <<<profile name>>>

ENTER AUTHORITY TO BE GRANTED:

ACCESS AUTHORITY  ===>    NONE, READ, UPDATE, CONTROL,
                          or ALTER

ENTER USER/GROUP ID TO BE ADDED:
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>

ENTER INFORMATION FOR PROFILE TO BE COPIED:

PROFILE NAME  ===>

CLASS         ===>

GENERIC       ===>    YES if the profile name is generic

VOLUME SERIAL ===>    If a non-cataloged data set profile
```

Enter the userid and the access you wish to assign to that person or group.

For Example:

To add the userid, SMITH, to the access list with READ authority to the profile USERID.PROJ,ONE, complete the screen as follows:

```
                    RACF - MAINTAIN DATA SET ACCESS LIST - ADD

COMMAND ===>

PROFILE NAME: <<<USERID.PROJ.ONE>>>

ENTER AUTHORITY TO BE GRANTED:

ACCESS AUTHORITY  ===> READ   NONE, READ, UPDATE, CONTROL,
                              or ALTER

ENTER USER/GROUP ID TO BE ADDED:
===> SMITH   ===>          ===>          ===>          ===>
===>         ===>          ===>          ===>          ===>
===>         ===>          ===>          ===>          ===>
===>         ===>          ===>          ===>          ===>
===>         ===>          ===>          ===>          ===>

ENTER INFORMATION FOR PROFILE TO BE COPIED:

PROFILE NAME  ===>

CLASS         ===>

GENERIC       ===>    YES if the profile name is generic

VOLUME SERIAL ===>    If a non-cataloged data set profile
```

For Example:

To add the userid, SMITH and the groupid GROUPA, to the access list with READ authority to the profile GROUPB.PROJ,ONE, complete the screen as follows:

```
                    RACF - MAINTAIN DATA SET ACCESS LIST - ADD

COMMAND ===>

PROFILE NAME: <<<GROUPB.PROJ.ONE>>>

ENTER AUTHORITY TO BE GRANTED:

ACCESS AUTHORITY  ===> READ   NONE, READ, UPDATE, CONTROL,
                              or ALTER

ENTER USER/GROUP ID TO BE ADDED:
===> SMITH    ===>          ===>          ===>          ===>
===> GROUPA   ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>

ENTER INFORMATION FOR PROFILE TO BE COPIED:

PROFILE NAME  ===>

CLASS         ===>

GENERIC       ===>    YES if the profile name is generic

VOLUME SERIAL ===>    If a non-cataloged data set profile
```

Task 24. Denying An Individual or a Group Use of A Data Set

SITUATION: You have a particular data set that a colleague who has left the department may still use. For security reasons you wish to exclude the person from using the data set.

Select the RACF option on the ISPF menu and RACF will display the following screen.

```
                        RACF SERVICES OPTION MENU

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                      for a DASD data set.

2 GENERAL RESOURCE    ADD, CHANGE, DELETE, or DISPLAY the
                      profile for a general resource.

3 GROUP               ADD, CHANGE, DELETE, or DISPLAY a group
                      profile.
                      CONNECT or REMOVE users.

4 USER                ADD, CHANGE, DELETE, or DISPLAY a
                      user profile.
                      Change a user's password.

5 SYSTEM OPTIONS      DISPLAY or SET the system wide
                      security options.
                      REFRESH in-storage profile lists.

T TUTORIAL            View a general description of RACF.
```

On the OPTION Line, enter 1. Press ENTER.

Option 1 gives you the following screen:

```
                        RACF - DATA SET SERVICES

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 ADD          Add a profile       D DISPLAY    Display profile
                                                contents

2 CHANGE       Change a profile    S SEARCH     Search RACF data
                                                set for profiles

3 DELETE       Delete a profile

4 ACCESS       Maintain access list

5 AUDIT        Monitor access attempts
                 (for auditors only)

ENTER DATA SET PROFILE INFORMATION:

PROFILE NAME        ===>

GENERIC             ===>   YES If the profile name is generic

VOLUME SERIAL       ===>   If the data set is not cataloged

UNIT                ===>   If option 1 and VOLUME SERIAL entered

DATA SET PASSWORD   ===>   If the data set is password protected
```

On the OPTION line, enter 4. Enter the profile name and any other appropriate information. Press ENTER.

Option 4 gives you the following screen:

```
                    RACF - MAINTAIN DATA SET ACCESS LIST

OPTION ===>

PROFILE NAME: <<<profile name>>>


SELECT ONE OF THE FOLLOWING:


1 ADD       Add users or groups, and/or
            Copy the access list from an existing profile.


2 REMOVE    Remove specified users or groups from
            the access list.


3 RESET     Remove all users and groups from the
            access list.
```

If you wish to remove ALL users or groups from the access list, on the OPTION line, enter 3. Enter the profile name. Press ENTER.

If you wish to remove only certain users or groups from the access list, on the OPTION line, enter 2. Enter the profile name. Press ENTER.

Option 2 gives you the following screen:

```
        RACF - MAINTAIN DATA SET ACCESS LIST - REMOVE
COMMAND ===>

PROFILE NAME: <<<profile name>>>

ENTER USER/GROUP ID TO BE REMOVED:

===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
```

Enter the userid(s) or groupid(s) you wish to remove from the access list.

For Example:

To remove userid, SMITH from the access list of the profile, USERID.PROJ.ONE, complete the screen as follows:

```
            RACF - MAINTAIN DATA SET ACCESS LIST - REMOVE
COMMAND ===>

PROFILE NAME: <<<USERID.PROJ.ONE>>>

ENTER USER/GROUP ID TO BE REMOVED:

===> SMITH    ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
```

Task 25. Removing Protection From Your Data Set

SITUATION: You have a data set containing experimental data which has been published. You no longer feel it is necessary to protect the data.

Select the RACF option on the ISPF menu and RACF will display the following screen.

```
                        RACF SERVICES OPTION MENU

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                      for a DASD data set.

2 GENERAL RESOURCE    ADD, CHANGE, DELETE, or DISPLAY the
                      profile for a general resource.

3 GROUP               ADD, CHANGE, DELETE, or DISPLAY a group
                      profile.
                      CONNECT or REMOVE users.

4 USER                ADD, CHANGE, DELETE, or DISPLAY a
                      user profile.
                      Change a user's password.

5 SYSTEM OPTIONS      DISPLAY or SET the system wide
                      security options.
                      REFRESH in-storage profile lists.

T TUTORIAL            View a general description of RACF.
```

On the OPTION Line, enter, 1. Press ENTER.

Option 1 gives you the following screen:

```
                        RACF - DATA SET SERVICES

OPTION ===>

SELECT ONE OF THE FOLLOWING:

1 ADD          Add a profile        D DISPLAY    Display profile
                                                 contents

2 CHANGE       Change a profile     S SEARCH     Search RACF data
                                                 set for profiles

3 DELETE       Delete a profile

4 ACCESS       Maintain access list

5 AUDIT        Monitor access attempts
                (for auditors only)

ENTER DATA SET PROFILE INFORMATION:

PROFILE NAME       ===>

GENERIC            ===>   YES If the profile name is generic

VOLUME SERIAL      ===>   If the data set is not cataloged

UNIT               ===>   If option 1 and VOLUME SERIAL entered

DATA SET PASSWORD  ===>   If the data set is password protected
```

On the OPTION line, enter 3. Enter the profile name and any other appropriate information. Press ENTER.

Option 3 gives you the following screen:

```
                                RACF - DELETE DATA SET PROFILE

COMMAND ===>

    PROFILE NAME:  <<<profile name>>>

    VOLUME SERIAL: <<<volume serial number>>>

ENTER/VERIFY INFORMATION BELOW:

    INDICATOR ===>      To turn the indicator off, enter SET
                        To leave indicator as is, enter NOSET


          To confirm delete request, press ENTER key.
          (The profile will be deleted.)


          To cancel delete request, enter END command.
```

Press ENTER.

Be careful when you delete a generic profile that you are not inadvertently removing RACF protection from a data set that should remain protected.

> CAUTION
>
> When you delete a data set profile, anyone (RACF-defined or not) can access, change, and/or delete your data set. You can selectively "remove" protection by selectively permitting or denying access to your data set. See Tasks 23 and 24 for detail.

MISCELLANEOUS TASKS

Tasks 26 through 30 are tasks you might need to perform occasionally, such as, copying, deleting or renaming a data set.

Task 26. Deleting A Data Set

If you have been entrusted with the authority to delete group data sets, be sure that all users of those data sets agree that a data set is no longer needed before you delete it.

To delete a data set, you must own the data set or have ALTER authority. If you know you are the owner or that you have ALTER authority, proceed with STEP 2.

STEP 1. Determining if you are owner or have ALTER authority

To find out if you have ALTER authority or if you are the owner, issue the LISTDSD command. Type:

LISTDSD DATASET('profile name') ALL

If the command fails, you will get a message stating you are not authorized. See your group/security administrator or owner.

If the command succeeds, you will see profile listing. Check the OWNER and the field, YOUR ACCESS in the profile listing. If you are the owner or you have ALTER authority, proceed with STEP 2. If you are not the owner or you do not have ALTER authority, see your group/security administrator or owner. If you need more information on how the data set is protected, see Task 5 (commands) or Task 18 (panels).

For example, to check the data set, **SMITH.PROJ.ONE**, type:

LISTDSD DATASET('SMITH.PROJ.ONE') ALL

STEP 2. Deleting the data set

To delete a data set, follow your standard deletion procedure. For example, under TSO, type:

DEL 'data set name'

If RACF does not permit you to delete the data set (the message under TSO SPF says "Deallocation failed"), you do not have the authority to delete the data set.

> CAUTION
>
> If you are deleting a data set protected by a generic profile, delete the data set not the profile.

To delete RACF protection from a data set, see Task 13 (commands) or Task 25 (panels).

Task 27. Moving Your Data Set

When you move a data set, the old data set is deleted. RACF does not permit you to move a data set unless you are the owner of the data set or you have ALTER authority to that data set. If you know you are the owner or that you have ALTER authority, proceed with STEP 2.

STEP 1. Determining if you are the owner of the data set or you have the ALTER authority

To find out if you have ALTER authority and the data set's owner, issue the LISTDSD command, type:

LISTDSD DATASET('profile name') ALL

If the command fails, you will get a message stating you are not authorized. See your group/security administrator or owner.

If the command succeeds, you will see profile listing. Check the OWNER and the field, YOUR ACCESS in the profile listing. If you are the owner or you have ALTER authority, proceed with STEP 2. If the field does not contain ALTER and you are not the owner, see your group/security administrator or owner. If you need more information on how the data set is protected, see Task 5 (commands) or Task 18 (panels).

For example, to check the data set profile, **SMITH.PROJ.ONE**, type:

LISTDSD DATASET('SMITH.PROJ.ONE') ALL

STEP 2. Moving the data set

To move a data set, use the utility you normally use.

CAUTION If you protected your data set with a discrete profile, your data set is not protected at the new location. You should consider protecting your data set at its new location. If you protected your data set with a generic profile, your data set is protected at the new location.

Task 28. Copying Your Data Set

Because a copy operation does not delete the original data set (as a move operation does) you can copy any data set for which you have READ authority. If you know that you have READ authority, proceed with STEP 2.

STEP 1. Determining if you have the READ authority

To find out if you have READ authority, issue the LISTDSD command. Type:

LISTDSD DATASET('profile name') ALL

If the command succeeds, you will see the profile listing Check the field, YOUR ACCESS in the profile listing. If you need more information on how the data set is protected, see Task 5 (commands) or Task 18 (panels).

If the command fails, you will get a message stating you are not authorized, see your group/security administrator or owner.

For example, to check the data set profile, **SMITH.PROJ.ONE**, type:

LISTDSD DATASET('SMITH.PROJ.ONE') ALL

STEP 2. Copying the data set

To copy a data set, use the utility you would normally use.

CAUTION

If you protected your data set with a discrete profile, your data set is not protected at the new location. You should consider protecting your data set at its new location. If you protected your data set with a generic profile, the copy of the data set may be protected at the new location , if the name of the copy matches the generic profile name.

Task 29. Renaming a Protected User Data Set

You can rename a protected user data set with the IEHPROGM utility, the access method services ALTER command, or the TSO RENAME command. However, the following rules apply:

- You must be the owner, have ALTER authority to the data set, or you must have the OPERATIONS or group-OPERATIONS attribute. (Use Task 2 (commands) or Task 15 (panels) to see what attributes you have.)
- You must have the authority required to create a new data set.
- You cannot rename a multivolume non-VSAM data set for which a discrete profile exists.
- You cannot rename a data set if the old name was covered by a generic profile and the new name is not.
- You cannot rename an individual member of a GDG if:
  - It is protected by a profile for the base portion of the GDG
  - The new data set name is a non-GDG name
  - No base profile has been defined.

    Note: To rename an individual data set name of a GDG, copy the data set to one having the new name.

If a discrete profile protects the old data set, the profile is changed to list you as the owner of the renamed data set. (Note: if you have the OPERATIONS or group-OPERATIONS attribute, this change does not take place. Instead, the user whose userid is the first-level qualifier of the renamed data set is made the owner.)

CAUTION
No change occurs in a generic profile protecting a data set that is being renamed. As a result of being renamed, a data set might be protected by a different generic profile than protected the old data set.

Task 30. Renaming a Protected Group Data Set

The same rules apply as for renaming a protected user data set. See Task 29 for details.

In addition, the following changes are made to a discrete profile for a renamed group data set:

- If you have the GRPACC attribute and the first-level qualifier of the old data set name is a group name, the group name is removed from the access list.

  Note: If the first-level qualifier of the *new* data set name is also a group name, that group name is added to the access list (as described under the next bullet).

- The access list is updated as follows: Your userid is added to the list and given ALTER authority (unless your id is already in the list, in which case, your authority remains unchanged). If you have the GRPACC attribute, the group indicated by the new name is added to the list and given UPDATE authority. The profile is also updated to show you as the owner of the data set (unless you have the OPERATIONS or group-OPERATIONS attribute, in which case the owner is not changed), and to show the current connect group as the one under which the data set was renamed.

CAUTION
As with user data sets, no change occurs to generic profiles protecting group data sets being renamed. As a result of being renamed, a data set might be protected by a different generic profile than applied to the old name.

Index

Resource Access
Control Facility
(RACF)
User's Guide

SC28-1341-0

READER'S
COMMENT
FORM

This manual is part of a library that serves as a reference source for systems analysts, programmers, and operators of IBM systems. You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Note: ***Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.***

Possible topics for comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name, company, mailing address, and date:

_____

_____

_____

_____

Note: Staples can cause problems with automated mail sorting equipment.
Please use pressure sensitive or other gummed tape to seal this form.

Cut or Fold Along Line

What is your occupation? _____

How do you use this publication? _____

Number of latest Newsletter associated with this publication: _____

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments or you may mail directly to the address in the Edition Notice on the back of the title page.)

Resource Access Control Facility (RACF) User's Guide

SC28-1341-0 S370-34

Reader's Comment Form

Cut or Fold Along Line

Fold and tape Please Do Not Staple Fold and tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 40 ARMONK, N.Y.

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Department D58, Building 921-2
PO Box 390
Poughkeepsie, New York 12602

Fold and tape Please Do Not Staple Fold and tape

Printed in U.S.A.

IBM®

Resource Access
Control Facility
(RACF)
User's Guide

SC28-1341-0

READER'S COMMENT FORM

This manual is part of a library that serves as a reference source for systems analysts, programmers, and operators of IBM systems. You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Note: ***Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.***

Possible topics for comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name, company, mailing address, and date:

_____

_____

_____

_____

Note: Staples can cause problems with automated mail sorting equipment. Please use pressure sensitive or other gummed tape to seal this form.

Cut or Fold Along Line

What is your occupation? _____

How do you use this publication? _____

Number of latest Newsletter associated with this publication: _____

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments or you may mail directly to the address in the Edition Notice on the back of the title page.)

Resource Access Control Facility (RACF) User's Guide

SC28-1341-0 S370-34

Reader's Comment Form

Cut or Fold Along Line

Fold and tape Please Do Not Staple Fold and tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 40 ARMONK, N.Y.

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Department D58, Building 921-2
PO Box 390
Poughkeepsie, New York 12602

Fold and tape Please Do Not Staple Fold and tape

Printed in U.S.A.

IBM®

Resource Access
Control Facility
(RACF)
User's Guide

SC28-1341-0

READER'S
COMMENT
FORM

This manual is part of a library that serves as a reference source for systems analysts, programmers, and operators of IBM systems. You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Note: ***Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.***

Possible topics for comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name, company, mailing address, and date:

_____

_____

_____

_____

Note: Staples can cause problems with automated mail sorting equipment.
Please use pressure sensitive or other gummed tape to seal this form.

Cut or Fold Along Line

What is your occupation? _____

How do you use this publication? _____

Number of latest Newsletter associated with this publication: _____

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments or you may mail directly to the address in the Edition Notice on the back of the title page.)

Resource Access Control Facility (RACF) User's Guide

SC28-1341-0 S370-34

Reader's Comment Form

Cut or Fold Along Line

Fold and tape Please Do Not Staple Fold and tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 40 ARMONK, N.Y.

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Department D58, Building 921-2
PO Box 390
Poughkeepsie, New York 12602

Fold and tape Please Do Not Staple Fold and tape

Printed in U.S.A.

IBM®

Resource Access
Control Facility
(RACF)
User's Guide

SC28-1341-0

READER'S
COMMENT
FORM

This manual is part of a library that serves as a reference source for systems analysts, programmers, and operators of IBM systems. You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Note: ***Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.***

Possible topics for comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name, company, mailing address, and date:

_____

_____

_____

_____

Note: Staples can cause problems with automated mail sorting equipment.
Please use pressure sensitive or other gummed tape to seal this form.

Cut or Fold Along Line

What is your occupation? _____

How do you use this publication? _____

Number of latest Newsletter associated with this publication: _____

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments or you may mail directly to the address in the Edition Notice on the back of the title page.)

Resource Access Control Facility (RACF) User's Guide

SC28-1341-0 S370-34

Reader's Comment Form

Cut or Fold Along Line

Fold and tape Please Do Not Staple Fold and tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 40 ARMONK, N.Y.

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Department D58, Building 921-2
PO Box 390
Poughkeepsie, New York 12602

Fold and tape Please Do Not Staple Fold and tape

Printed in U.S.A.

IBM®