Forest Service Handbook
National Headquarters - Washington Office
Washington, DC

Forest Service Handbook 6609.11 – System Management Handbook
Chapter 10 - Access Management

Amendment: 6609.11-1991-1

Effective date: September 03, 1991

Duration: This amendment is effective until superseded or removed.

Approved by: F. Dale Robertson, Chief

Date approved:

Responsible Staff:

Last Change:

Superseded Document(s): Title Page; 00--1 thru 53; 5, April 1989; 4, July 1988

Digest: Following is an explanation of the changes throughout the directive by section.

This amendment is a reissuance of FSH 6609.11 to conform the format and structure of the Handbook to the requirements of electronic directive issuance.

This amendment makes no substantive changes to the text. The only changes made are those necessary to meet new format requirements or to correct spelling, punctuation, or unit names.

This Handbook is now available electronically in the National Information Center in the same format as the paper copy. Henceforth, amendments to this Handbook will be issued to Forest Service units electronically on a document basis.

Table of Contents

10.3 - Policy

1. Do not change the two standard Preditor user profiles (USER and PRIV_USER). All passwords must be encrypted, and all users must have :FSIA:MODULES:AM.PR as their initial program.

2. Establish a process for creating user profiles that fits the needs of each organizational location.

3. Identify each person as a Data General user at one office only. The exception to this rule is limited to allowing an authorized person at one location to log on with a privileged profile at another office to provide system management support.

4. Do not give passwords to other users. Each individual user must supply a username/password pair, that is known only to that person, to log on to a Data General system. This rule also applies to the use of guest and privileged profiles. System users must not give their personal passwords to any other user for any reason.

5. Assign standard user privileges to all Forest Service employees assigned to the local site. Assign superuser profile privileges only to those who must have those privileges to carry out their responsibilities.

6. Establish organizational unit usernames so that units and subunits can receive mail and file material in their areas of responsibility. Include the MAILROOM and FILECLERK (to maintain files) as functional usernames.

7. Change the password for a GUEST profile when it is no longer needed by the guest to whom it was assigned so that no one can access the system with the profile until it has been reassigned to another guest user.

8. Set up remote aliases for line officers.

11 - Local Access to Local Host

11.1 - Granting Access

Access to USDA and Forest Service information processing facilities may be granted to all appropriate Forest Service personnel. Access by non-Forest Service personnel (for example, State, Local, or other government agencies) may be granted where such access complies with FSM 6607.

11.11 - Process

Responsible Official	Action
Unit Manager (Staff Director, Forest Supervisor, District Ranger)	1. Notifies group responsible for system management of the names of the users allowed access to the computer system.
	2. Provides information necessary to establish profiles.
Director of Systems Staff	3. Completes and signs the profile approval for Designated each of the requested names.
System Manager	4. Creates the appropriate Preditor profile.
	5. Assigns a randomly-generated password (minimum six characters) to prevent users from logging onto the system before the profile is fully established.
	6. If the profile is for an individual user, coordinates with official having edit privileges to the People Database to enter the new user into the database.
	7. Gives the randomly-generated password to the official assigned the Comprehensive Electronic Office (CEO) management responsibilities.
CEO Manager	8. Creates the CEO Profile (see section 11.42).
	9. Sends a CEO mail message to the new user to confirm the user's aliases.
System Manager	10. Executes a macro (:FS:CEO_SPACE_SET.CLI) to limit the user's CEO space according to the management decision at the site.
	11. Notifies user of the initial password for the profile and encourages the user to change the password immediately and on a regular basis thereafter.
	12. Encourages user to log off the system when the terminal is unattended.

11.12 - Access Privileges

To ensure management that the confidentiality of office materials is protected when processed and stored by the computer systems, special rules are necessary for governing access privileges. These rules are:

1. Assign privileges of superuser and superprocess only to those who need them to carry out their responsibilities. Typically, one to three people per system need these privileges. The superuser and superprocess privileges must not be part of the user profile for non-managers of the system.

2. Do not allow use of the privilege "Change Username"; it is unnecessary if the following rules are followed:

   a. Perform operator functions only at the operator console. Keep the console in "LOCK_CLI" status between these operations.

   b. When performing work for another person, the system manager should ask that person to sign on and allow the system manager to use the terminal.

3. Each user with superuser and superprocess privilege must have two profiles. Because of the risk involved in leaving a superuser signed on while no one is at a terminal, use the following method for dealing with superuser profiles:

   a. Ensure that:

   (1) The first profile does not have the superuser and superprocess privileges;

   (2) The first profile has modem privileges; and

   (3) The first profile is the profile that is used for that person's normal work, including CEO.

   b. Create another profile which has superuser and superprocess privileges, but not modem or other remote privileges. This profile exists for times when privileges are necessary. The user signs on with this profile for special purposes only, and then signs off.

The following is an example:

Userid	Privileges
L.USER	The usual list contained in the profile named USER (see section 11.41a).
$L.USER	The usual list contained the profile named PRIV_USER (see section 11.41b).

Persons who have superuser profiles must never, under any circumstances, give their passwords to others.

5. System personnel shall not keep records of current passwords. If access to a user's data is needed when the user is unavailable, and it is absolutely necessary for the system manager or another user to sign on as that user, the system manager should change the password using Preditor. When the users returns, the system manager should inform the user of the password change and ask the user to log on and enter a new password. Use of this procedure assures users that access to the system is secure from abuse. This procedure must only be used in cases of emergency and only under the direction of management.

11.2 - Classes of Users

The types of users allowed to access the system can be grouped into the following classes:

1. Individual. Members of this class are distinguished by the condition that each user is identified as a single person. The majority of the user community has membership in this class.

2. Organizational Units and Functional Users. Profiles are established for organizational subunits so that they can receive mail and file material in their areas of responsibility. Organizational unit names have their own private files to represent that unit. The unit "users" handle routing and approval of documents within the unit, sending of official documents, and filing of records material; creation and editing of documents is usually performed by an individual user. Each unit that receives mail must be represented with a username which functions as a mail stop.

Functional users are those which provide a necessary service, but cannot be represented as a subunit. Two required functional users are Mailroom and Fileclerk. The Mailroom function is used for the orderly transfer and distribution of mail and documents to the proper organization units. The Fileclerk function facilitates centralized filing of records (correspondence and other record material).

Users in this class only have access to the CEO environment.

3. Privileged. Users in this class are limited to those individuals (OP and $ Users) who have been assigned system management and operation responsibilities. OP should be assigned a CEO for word processing, electronic mail, or other non-CEO management tasks. Privileged users other than OP must not have a CEO profile.

4. Guest. Users who are not a part of the local user community, but require temporary access to the local system, are members of this class. A GUEST profile must be established in all cases where temporary access is required. Local user community members must not log on for, or give their passwords to, guest users.

5. Special. Users who need to have permanent access to the system, but cannot be represented by any of the above classes, belong to this class. Examples of this class include the TIMER profile which is used to measure CEO performance, and the HOME profile which allows visitors to access their home systems.

11.3 - User Identification and Aliases

To access the DG computer system, all users must have a username and password. Additionally, users with access to the Comprehensive Electronic Office (CEO) are provided with: an inbox, calendar, and file cabinet; the ability to create, edit, file, and send messages and documents; and support for other office and decision making procedures. Users allowed access to CEO must also have a CEO Username and up to three CEO aliases to be recognized by the system.

Within a system node, each username and alias must be unique. A username can consist of up to 15 characters, but cannot contain blanks. When a username exceeds 15 characters, the name must be abbreviated by removing vowels from right to left, followed by the removal of consonants in the same manner if necessary. CEO username and aliases can be as long as 18 characters, and may contain blanks. In cases where a CEO username or alias exceeds 18 characters, the username or alias must be abbreviated by using initials in the place of middle and then first names.

The following discussion includes brief examples of user identification and aliases by user type. Refer to section 16, exhibit 01 for a more detailed list of examples.

11.31 - Username

11.31a - Individual Users

An individual's username consists of an initial and the last name, separated by a period (.). For example:

Individual's Name	System Username
Theodore Roosevelt	T.Roosevelt
Gifford Pinchot	G.Pinchot

In cases where this convention creates a username duplication, another initial, such as a middle initial, can be used to make the names unique. For example:

Individual's Name	System Username
Smokey The Bear	S.T.Bear
Smokey Bear, Jr.	S.Bear

11.31b - Organizational/Functional, Guest and Special Users

Usernames for organizational subunits and functional users must not contain a period (.) in either of the first or second positions. All guest users names must begin with GUEST, followed by up to 10 characters that assures the name be unique. Special usernames are assigned by FSIA system developers.

11.31c - Privileged Users

All users in this class must first have an individual profile. The username for a privileged user will be the same as that used for the user as an individual preceded by the dollar sign ($) character. For example:

Individual's System Username	Privileged Username
S.Bear	$S.Bear

If the privileged username exceeds 15 characters, the username must be abbreviated as explained above. The privileged username without the preceding $ must be the same as the standard username for the user.

11.32 - CEO Username

Since the CEO system uses the username as a signature on letters, use the user's name as it would appear on signed letters. For example:

Smokey T Bear

11.33 - CEO Alias

At least one alias must be created for individual and organizational/functional users. The first alias is used to enter the user into the user directory. The format for this first alias is: last

name, comma (,), space, first name, space, and middle initial(s). Use the remaining aliases as desired. For example:

First CEO:	Bear, Smokey T
Remaining Alias:	Smokey

11.34 - Remote Alias

Remote aliases make it easier to send mail and informal correspondence to other network nodes. Set up remote aliases for the line officers of the parent unit and all subordinate units. The standard for remote aliases is the common name, followed by the initial of the last name. For example:

Individual's System Username	Remote Alias
S.Bear	Smokey B

11.35 - Executive Communication System

The executive communication system has been set up to facilitate communication among Regional Foresters, Station Directors, and the Area Director. For those sites that need to utilize this system, remote aliases shall be set up for: the Chief, Associate Chief, Deputy Chiefs, Associate Deputy Chiefs, Regional Foresters, and Station and Area Directors.

11.4 - Profile Types

There are three profile types which must be maintained on the system: the Preditor profile, which allows access to the system; the CEO profile, which allows access to CEO; and the People Data Base profile. Section 16, exhibit 02 contains a quick reference of allowable profile types by user class.

11.41 – Preditor
Do not change the two (USER and PRIV_USER) profiles on the system. Use the appropriate profile as a default when establishing new users. All users must have :FSIA:MODULES:AM.PR as the initial program.

11.41a - Individual, Organizational/Functional, Guest and Special User Profile

Use the "USER" profile displayed in section 16, exhibit 03 when establishing these users on the system.

11.41b - Privilege Profile

Use the "PRIV_USER" profile displayed in section 16, exhibit 04 when establishing these users on the system. Due to the additional user accountability afforded by AM, the standard settings may be changed to "Yes", as directed by management, for the following privileges:

1. Use virtual console [Yes]
2. Modem [Yes]

11.42 - CEO

11.42a - Profile Menu

The menu to create or edit a given CEO Profile is displayed in section 16, exhibit 05. Use the conventions described in section 11.3 for user ID, username and aliases. Make sure to place the first alias in the directory. The use of the user data fields is optional. The names of these fields may be changed depending on management direction; suggested names are: Phone, Room, Staff and Other. Use the following to guide responses to the other profile items:

1. Allow use of CLI? (Y/N) N - Optional.

2. CEO Management Privileges? (Y/N) N - Answer "Y" only for those users who have been assigned CEO management responsibilities.

3. External mail privileges? (Y/N) N - This feature is not available.

4. Type of access to User Applications: 3 (Public) - Optional. The use of options "None" and "Personal" is not permitted. Management may elect to grant access to "Both" Public and Personal for individual or guest users; access for all other user classes is limited to Public. Personal applications are limited to those routines which restrict data manipulations to files in the user's IS_CEO/IMPORT_EXPORT Drawer/Folder.

5. Is this user exempt from automatic archiving? (Y/N) N - Optional. This option is only relevant when automatic archiving is utilized. If automatic archiving not invoked, this item is ignored.

6. Use systemwide inactive time period for automatic archiving? (Y/N) Y - Optional. This item is only relevant when automatic archiving is utilized.

7. Use confidential mail? (Y/N) Y - Required.

8. Use certified mail? (Y/N) Y - Required.

9. Use urgent mail? (Y/N) Y - Required.

10. Use eyes only mail? (Y/N) Y - Required.

11. Send mail on behalf of other users? (Y/N) Y - Required.

11.42b - CEO Personal Profile

CEO allows the users to make selected changes to their CEO profiles. Encourage the user community to make changes in their profiles as is appropriate to suit their needs. All CEO users must have access to the Public cabinet.

11.42c - CEO Commands

The CEO manager creates initial CEO user commands to assist users while they are performing tasks in the CEO environment.

1. Required Commands:

    a. Leave the CEO System

    Command Name: F1
    Command Description: Leave the CEO System
    Starts from: Main Menu
    Command Content: (ESC) CANCEL/EXITy NEW LINE (ESC)

    b. Return to CEO Main Menu

    Command Name: F2
    Command Description: Return to CEO Main Menu
    Starts from: Main Menu
    Command Content: (ESC) (ESC)

    Note: There is no content for this command other than the beginning and ending command delimiters (ESC).

2. Optional Commands:

    a. View Inbox

    Command Name: F3
    Command Description: View Inbox
    Starts from: Main Menu
    Command Content: (ESC) NEW LINE NEW LINE (ESC)

b. Enter Calendar Function

Command Name: F4
Command Description: Enter Calendar
Starts from: Main Menu
Command Content: (ESC) 6 NEW LINE (ESC)

c. Enter IS Environment

Command Name: F5
Command Description: Enter IS
Starts from: Activity where invoked
Command Content: (ESC) INTERRUPT7 NEW LINEIS NEW LINE1 NEW LINE (ESC)

Optional commands like those shown above can be placed on any of the function keys other than F1 and F2. Others may be added at the user's discretion.

11.5 - People Database Entry

All individual users must have an entry in the People Database to access the system via their personal, privileged or organizational/functional profiles. The FSIA AM server will terminate an access attempt by any user if there is no entry for the individual in the People DB. Coordinate with the official having edit access to the People DB to make sure that all individuals have the required entry.

11.6 - Global Privileged Password Management

The privileged password is managed through the Change Global Privileges option of the System Management Functions Menu option of the FS System Manager Functions Menu (see section 16, exhibit 06). As with all passwords, the privileged password shall be changed at regular intervals to maintain system security.

11.7 - Guest Profile Password Management

The system manager is responsible for the management of all GUEST user profile passwords. When a particular GUEST profile is no longer needed by the guest to whom it was assigned, the system manager must change the password. This procedure will ensure that no one can access the system with the profile until it has been reassigned to another guest user.

12 - Remote Access to Local Host

12.1 - Communications Hardware Management

12.11 - Remote Diagnostic Device Access

There are currently three devices furnished by Data General which provide access (via modem) to a CPU for remote diagnostic purposes: Comswitch I, Comswitch II, and the Diagnostic Remote Processor (DRP). The Comswitches are external devices, and the DRP's are internal devices on newer CPU's such as the MV/7800, MV/15000 and MV/20000. Since access via these devices allows full control of the system and system console and thereby poses a significant security risk, the following standards shall be adhered to by all Forest Service sites:

1. All systems with a DRP shall have the Machine Initiated (MI) call-out feature ENABLED, and the MI call-out number set to RAC's standard number. (Note - Only the Field Engineer (FE) can do this.)

2. All systems with a Comswitch II or DRP shall use the password feature. The password shall be at least eight characters, both alpha and numeric, in a random or meaningless pattern. Since an operator must be present to provide modem access, it is not necessary for anyone to remember this password. The operator should view it (BRK,'A') and provide it to the person needing access. The password shall be changed immediately after any remote access.

Section 16, exhibit 07 shows the proper procedure to follow when RAC needs access to a system with a DRP. Systems with a Comswitch II should follow a similar procedure with the only change being in the method of enabling/disabling the modem.

3. All systems with a Comswitch II or DRP shall have the RAC call back number stored (BRK,'J'). Other (FS) call back numbers may be stored also.

4. Except when the Remote Assistance Center (RAC) or a Forest Service help desk is accessing the device, the modem shall be prevented from automatically answering calls and giving access to the device in one of the following ways:

(a) Comswitch I - Turn off the modem or physically disconnect the phone line from the modem. In addition, the switches on the device must be set to POWER OFF.

(b) Comswitch II - Turn off the modem or physically disconnect the phone line from the modem. In addition, the keyswitch must be set to NONE. (If turning the modem off causes the device to display an error message on the master console, turn the keyswitch to LIMITED, then back to NONE).

(c) DRP - Set the (DG supplied) modem to NO ANSWER by turning dip switch 5 (on the bottom of the modem) to OFF (Down), then turning the modem off and back

on. The modem must remain on and connected to the phone line for the MI feature. In addition, the Access Level must be set to NONE via the master console (BRK Q).

5. Under no circumstances leave a Comswitch I, Comswitch II or DRP enabled for outside access, except when the RAC or Forest Service Help Desk is actively utilizing the device and a representative for the local site is in attendance.

6. Do not connect anything to the Comswitch or DRP user ports (J4 on the Comswitch I, P4 and P5 on the Comswitch II, and User Terminal and User IAC on the DRP).

12.12 - Comswitch Access

In addition to the Comswitch standards set in section 12.11, sites that wish to make use of the modem and phone line associated with the Comswitch for user access to the system may do so by following the diagram in section 16, exhibit 08.

12.13 - Modems on a Local Area Network (LAN)

Modems connected to a LAN, telephone switch, port selector, or front-end devices shall not be allowed to access IAC-16 ports or IAC-8 ports configured as non-modem-controlled. If the front end device connects a modem to an IAC-8 port configured as modem controlled, the device must pass all modem control signals between the modem and IAC-8 port. These limitations are necessary to allow AM to apply additional security requirements to system access from remote locations.

12.2 - Global Non-local Password Management

The non-local password is designed to provide a means for a site to stop access to the local system by remote users. The password is set with the appropriate Global Privilege (see section 16, exhibit 06). Under normal circumstances, the password is set and shared with local employees so that it will be easy for them to use to access their local system when they are visiting another Forest Service office.

12.3 - Deflected Access Management

12.31 - Global Deflected Access Privilege

The System Manager allows use of deflected drawers by setting the appropriate Global Privilege (see section 16, exhibit 06). Normally, deflection is allowed at all times and is only turned off during unusual circumstances.

12.32 - Allowing Remote Nodes Access to Local Deflected Drawers

In order for a remote node to use deflected drawers on the local system, the local System Manager must allow deflected access to that remote node (see section 16, exhibit 06, Deflected Access).

13 - Local Access to Remote Hosts

13.1 - Global Access to Remote Hosts Privilege

The System Manager allows access to remote hosts by local users by setting the appropriate Global privilege (see section 16, exhibit 06). This access can be removed in the event of unexpected circumstances that necessitate restricting access.

13.2 - Management of Home Profile

The HOME profile (see section 11.2) is created by the local System Manager for use by visiting employees. Since this is a privilege which is provided for guests, it is the System Manager's responsibility to manage how this privilege is granted. The objective of the management of this profile is to prevent unauthorized guests having access to system resources without having been granted the privilege to do so.

The best way to manage this privilege is by managing the HOME password. Keep the password simple, at least 6 characters long, and well known to the local user community.

To effectively manage the HOME password, the Change Password privilege of the HOME Preditor Profile must be removed. To do this, execute Preditor and edit the HOME profile. At the prompt, "Change Password", enter "N". This will prevent guests utilizing the profile from being able to modify the password. It will then be necessary to execute Preditor each time the password for the HOME profile is to be changed.

13.3 - Department Computer Center (DCC) Access

The System Manager allows access by users to the various USDA Computer Centers by managing DCC access (see section 16, exhibit 06). The Washington Office CS&T Staff (through Regional Coordinators) will provide site ID's and passwords for access to Department Computer Centers (for example, Fort Collins Computer Center and National Finance Center).

14 - Network System Management

14.1 - Network Management Functions

Network management consists of two broad but distinct management functions. They are:

1. Establishing and maintaining XODIAC and Remote Job Entry (RJE) configuration and program files.

2. Establishing, maintaining, and ensuring proper performance of local data communications facilities, such as modems, switches, and similar devices, and maintaining liaison with Telenet and the concerned public telephone utility.

The Washington Office Computer Sciences and Telecommunications (CS&T) staff manages data communication network services provided through the Department of Agriculture's contract (DEPNET) with Telenet. Computer and Telecommunication System Managers are responsible for requesting normal repair services directly from the contractor. All other liaison with the vendor will be performed by the Washington Office Telecommunications staff. This includes network status requests, ordering services, major repairs, billing, documentation, and technical inquiries.

14.2 - Unique Identifiers

The node naming convention, in conjunction with usernames, insures that each Forest Service employee is uniquely identified on the network. Refer to section 11.3 for username standards and section 33.1 for the node name standards. There are cases where different Forest Service organizational units are sharing machines, thereby creating dual-designated systems. These systems will have two node names. At the site's choice, one of the node names shall be specified as the local host name in the processor's NETGEN (see section 33.1).

14.3 - Access for Non-Forest Service Sites

Refer to section 33.2.

14.4 - Transfer of Information between Nodes on the Network

CEO Mail is the simplest and easiest method to send official mail, personal notes, and small non-CEO files to users on remote nodes. Do not use CEO Mail for transferring large files between nodes. These should be exported and sent via the RIS utility.

The transfer of non-CEO data files from one system to another is accomplished by using "Retrieval" (RIS), a feature in the IS utilities. Only Public or Staff files can be transferred through the network using this utility. Files can only be transferred to/from drawers which have been set for RIS access by the Staff or Public Information Managers. Retrieval requires that the users who are sending information to an account on a remote node must notify the remote user via CEO that the file is available for retrieval, giving the Level (Public or Staff cabinet), Drawer, Folder and Object names.

To use the network cost-effectively, System Managers should encourage users to schedule file transfers for the period 6:00 PM to 6:00 AM when network costs are lowest. Additionally, this

will assist in balancing the network workload by doing file transfers when CEO Mail is likely to be least active.

15 - Management of Access to Public And Staff is Cabinets

Refer to Section 43 for information on the structure of these IS areas. The IS system requires that specific usernames be given management responsibilities for the Public and Staff cabinets. The System Manager is responsible for ensuring that a management decision is made regarding which person(s) should assume these duties for the local site (refer to FSM 6620). It may not be appropriate to assign all aspects of public and/or staff cabinet management to a single organizational group or individual. One or more Public Information Managers must be designated and assigned these duties within the IS system. One or more Staff Information Managers must be designated for each staff created on the system.

15.1 - Assignment of Public and Staff Information Managers

Once the unit's information managers have been selected, the System Manager will assign the duties to those persons with the "Information Managers" activity (see section 16, exhibit 06).

15.2 - Establishment of Staff Cabinets

Staff information is generally best organized and managed by following the existing staff group organization at the local site. The System Manager should establish specific staff groups and areas within the IS system using the "Staff Directories" activity (see section 16, exhibit 06). Each staff is responsible for the maintenance of the information stored in the their respective staff cabinet.

16 - Exhibits

16 - Exhibit 01

Examples of User Identification and Aliases

Individual User:

System Username	Primary Alias	Secondary Alias
S.Bear	Smokey T Bear	Bear, Smokey T

Organizational User:

System Username	Primary Alias	Secondary Alias
Washington Office:		
Chief	Office of Chief	Chief, Office of
PL	Deputy Chief, P&L	P&L, Deputy Chief
OI	Director, OI	OI, Director
Regional Office:		
RF	Regional Forester	
Admin	Deputy RF, Admin	Admin, Deputy RF
FAM	Director, F&AM	F&AM, Director
Supervisor's Office:		
FS	Forest Supervisor	
Rec	Staff Officer, Rec	Rec, Staff Officer
District Office:		
DR	District Ranger	

Functional User:

System Username	Primary Alias	Secondary Alias
Mailroom	Mail	Mail Room
Fileclerk	File Clerk	Public Files

Guest User:

System Username	Primary Alias	Secondary Alias
Guest1		

16 - Exhibit 02

Profile Types by User Class

User Class	AOS/VS Profile	CEO Profile	People Data Base Profile
Individual	USER	Yes	Yes
Organizational/ Functional	USER	Yes	No
Privilege	PRIV_USER	No	No
Guest	USER	Yes	No
Special	Assigned as needed by FSIA System developers.		

16 - Exhibit 03

Preditor Profile for all Non-Privileged Users

```
Username: USER
Encrypt password [Yes]
Initial IPC file []
Program [:FSIA:MODULES:AM.PR]
Create without block [Yes]
Use IPC [Yes]
Use console [Yes]
Use batch [Yes]
Use virtual console [Yes]
Access local resources from remote machines [Yes]
Change password [Yes]
Unlimited sons [Yes]
Change priority [No]
Change type [No]
Change username [No]
Access devices [No]
Superuser [No]
Superprocess [No]
System Manager privilege [No]
Modem [Yes]
Change address space type [Yes]
Change working set limit [Yes]
Priority [2]
Max qpriority [0]
Disk quota [500]  - *       Maximum number of 512 byte disk
                            blocks the user has in the CLI
                            environment.  The value is
                            installation dependent.
Logical address space       - batch    [-1 system default]
Logical address space                  - non-batch [-1 system default]
Minimum working set size               - batch    [-1 system default]
Maximum working set size               - batch    [-1 system default]
Minimum working set size               - non-batch [-1 system default]
Maximum working set size               - non-batch [-1 system default]
Default user locality - non-batch [0]
Use other localities - non-batch [No]
Default user locality - batch [0]
Use other localities - batch [No]
User comment []   - *       Recommend using this field to enter
                            the date profile is assigned and
                            initials of person running the
                            Preditor program.
```

16 - Exhibit 04

Preditor Profile for Privileged Users

Username: PRIV_USER
Encrypt password [Yes]
Initial IPC file []
Program [:FSIA:MODULES:AM.PR]
Create without block [Yes]
Use IPC [Yes]
Use console [Yes]
Use batch [Yes]
Use virtual console [No]
Access local resources from remote machines [No]
Change password [Yes]
Unlimited sons [Yes]
Change priority [No]
Change type [No]
Change username [No]
Access devices [No]
Superuser [Yes]
Superprocess [Yes]
System Manager privilege [No]
Modem [No]
Change address space type [Yes]
Change working set limit [Yes]
Priority [2]
Max qpriority [0]
Disk quota [1000] - * Maximum number of 512 byte disk blocks the user has in the CLI environment. The value is installation dependent.
Logical address space - batch [-1 system default]
Logical address space - non-batch [-1 system default]
Minimum working set size - batch [-1 system default]
Maximum working set size - batch [-1 system default]
Minimum working set size - non-batch [-1 system default]
Maximum working set size - non-batch [-1 system default]
Default user locality - non-batch [0]
Use other localities - non-batch [No]
Default user locality - batch [0]
Use other localities - batch [No]
User comment [] - * Recommend using this field to enter the date profile is assigned and initials of person running the Preditor program.

16 - Exhibit 05

CEO Profile Menu

USER'S SYSTEM PROFILE

		In Directory?	Global?
User ID:	**S.Bear**	**N**	**N**
User Name:	**Smokey T Bear**	**N**	**N**
Aliases:	**Bear, Smokey T**	**Y**	**N**
	Smokey	**N**	**N**
	Smokey Bear	**N**	**N**

Phone:
Room:
Staff:
Other:

Do you want to modify user privileges? (Y/N) **Y**

Execute? (Y/N)

USER PRIVILEGES MENU

User Name: **Smokey T Bear**

Allow use of CLI?(Y/N) **N** CEO Management Privileges?(Y/N) **N**
External mail privileges? (Y/N) **N**

Type of access to User Applications:
(1. None, 2. Personal, 3. Public, 4. Both) **3**

Is this user exempt from automatic archiving? (Y/N) **N**
Use systemwide inactive time
period for automatic archiving? (Y/N) **Y**

Use confidential mail? (Y/N) **Y** Use certified mail? (Y/N) **Y**
Use urgent mail? (Y/N) **Y** Use eyes only mail? (Y/N) **Y**
Send mail on behalf of others? (Y/N) **Y**

Execute? (Y/N)

16 - Exhibit 06

System Management Functions Menu

Menu item:	Purpose:
1. Staff Directories	Establishes, views, changes, or deletes staff information cabinets.
2. Information Managers	Add or delete staff and public information managers.
3. Deflected Access	Add, delete or view remote nodes that currently have deflected access to the local system.
4. Global Privileges	Sets the global privileges: remote system access, deflected drawer access, non-local password, privilege password.
5. Manage DCC Profiles	Establishes access by username to Departmental Computer Centers.

16 - Exhibit 07

RAC Access Procedure For Systems With a DRP

1. Place the call to RAC.

2. While you are waiting for them to call back:

   (a) At the master console, hit 'Break' (CMD/BREAK if a VT)

   (b) When you see *** SYSCON BREAK ***, hit 'A'. This will display the current password.

   (c) Type 0 <NL> to exit.

   (d) Hit break or CMD/BREAK again.

   (e) When you see *** SYSCON BREAK *** hit 'Q'. It should display 'Access Level None'.

   (f) Type 1<NL>, 1<NL> to change the access level to 'Full'.

   (g) Type 0 <NL> to exit.

   (h) Set the RAC modem to Auto Answer: Turn the modem over and set dip switch 5 to 'on' (up). Turn the modem off and back on.

3. If RAC needs access when they call back, give them the password you found above and the modem phone number.(Note: They will call in, give the password, and leave their phone number. If the phone number they leave matches one stored in the DRP, the system will call them back. You'll see all this on the console).

4. After RAC is completely done and no longer needs access:

   (a) Set the modem to No Answer: Turn the modem over and set dip switch 5 to 'off' (down). Turn the modem off and back on.

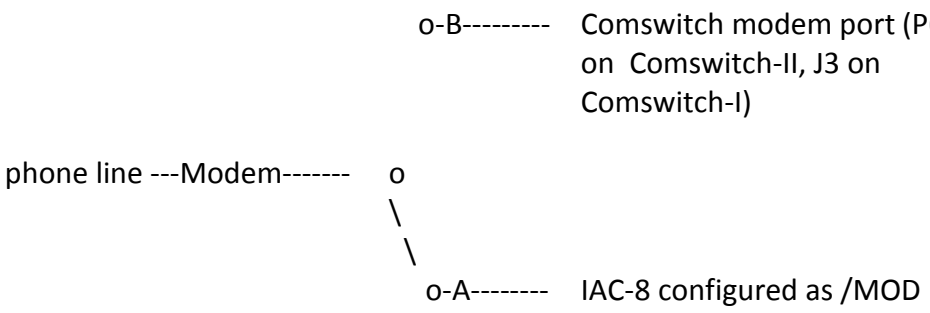
   (b) At the master console, hit break (or CMD/BREAK) Q, 1 <NL>, 1<NL>, 0<NL> to set the access level back to none.

   (c) Hit break (or CMD/BREAK) again, then A, 1<NL>. You will then be prompted to enter a new password. Key in at least 8 alpha and numeric characters of your own choosing in a random or meaningless pattern, followed by <NL>. (No one has to remember this one). Then type 0<NL> to exit.

16 - Exhibit 08

Sharing a Comswitch Phone Line and Modem

Sites that wish to make use of the modem and phone line associated with the Comswitch for user access to the system may do so by obtaining an RS-232 A-B switch and connecting it in the following manner:



The switch shall be left at "A" except when RAC or the Forest Service Help Desk is actually accessing the Comswitch. This is an acceptable way to meet the requirement of preventing a a Comswitch I or Comswitch II from answering calls.
