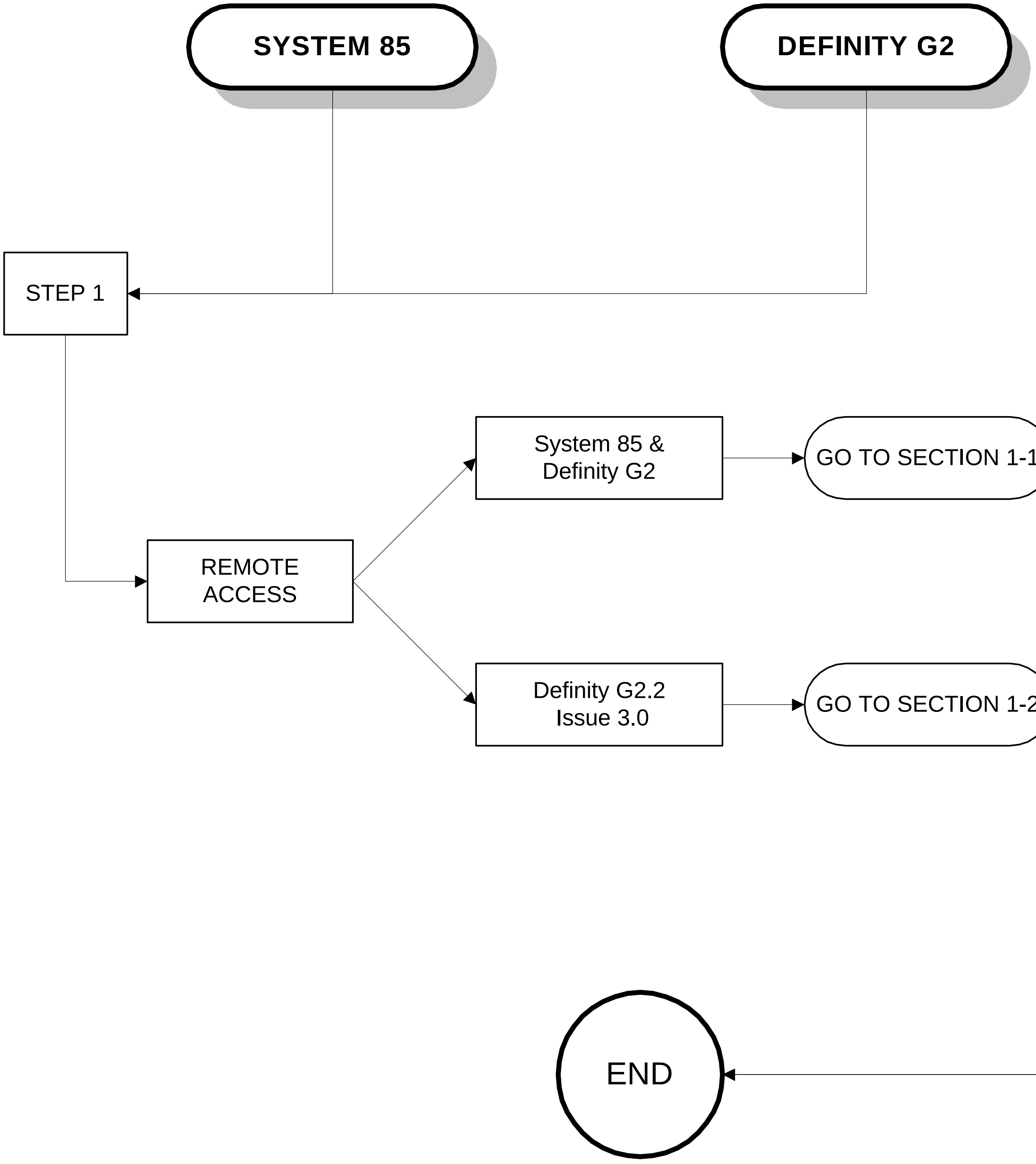
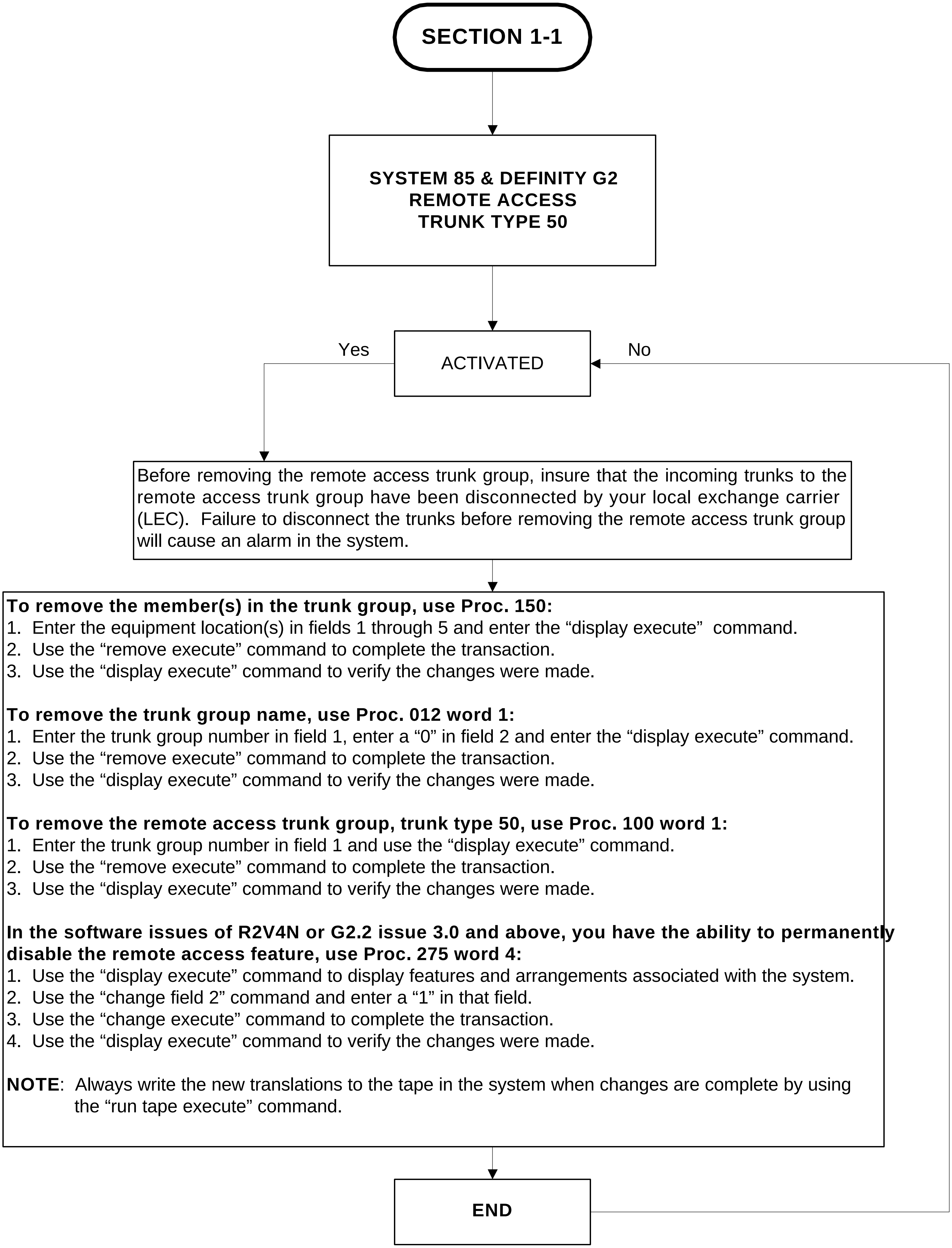
AT&T
SYSTEM SECURITY
CERTIFICATION

SYSTEM 85
DEFINITY G2
DEFINITY G2.2

SYSTEM SECURITY CERTIFICATION

THE FOLLOWING FLOW CHART MUST BE FOLLOWED IN ITS ENTIRETY





Before removing the remote access trunk group, insure that the incoming trunks to the remote access trunk group have been disconnected by your local exchange carrier (LEC). Failure to disconnect the trunks before removing the remote access trunk group will cause an alarm in the system.

To remove the member(s) in the trunk group, use Proc. 150:

1. Enter the equipment location(s) in fields 1 through 5 and enter the “display execute” command.
2. Use the “remove execute” command to complete the transaction.
3. Use the “display execute” command to verify the changes were made.

To remove the trunk group name, use Proc. 012 word 1:

1. Enter the trunk group number in field 1, enter a “0” in field 2 and enter the “display execute” command.
2. Use the “remove execute” command to complete the transaction.
3. Use the “display execute” command to verify the changes were made.

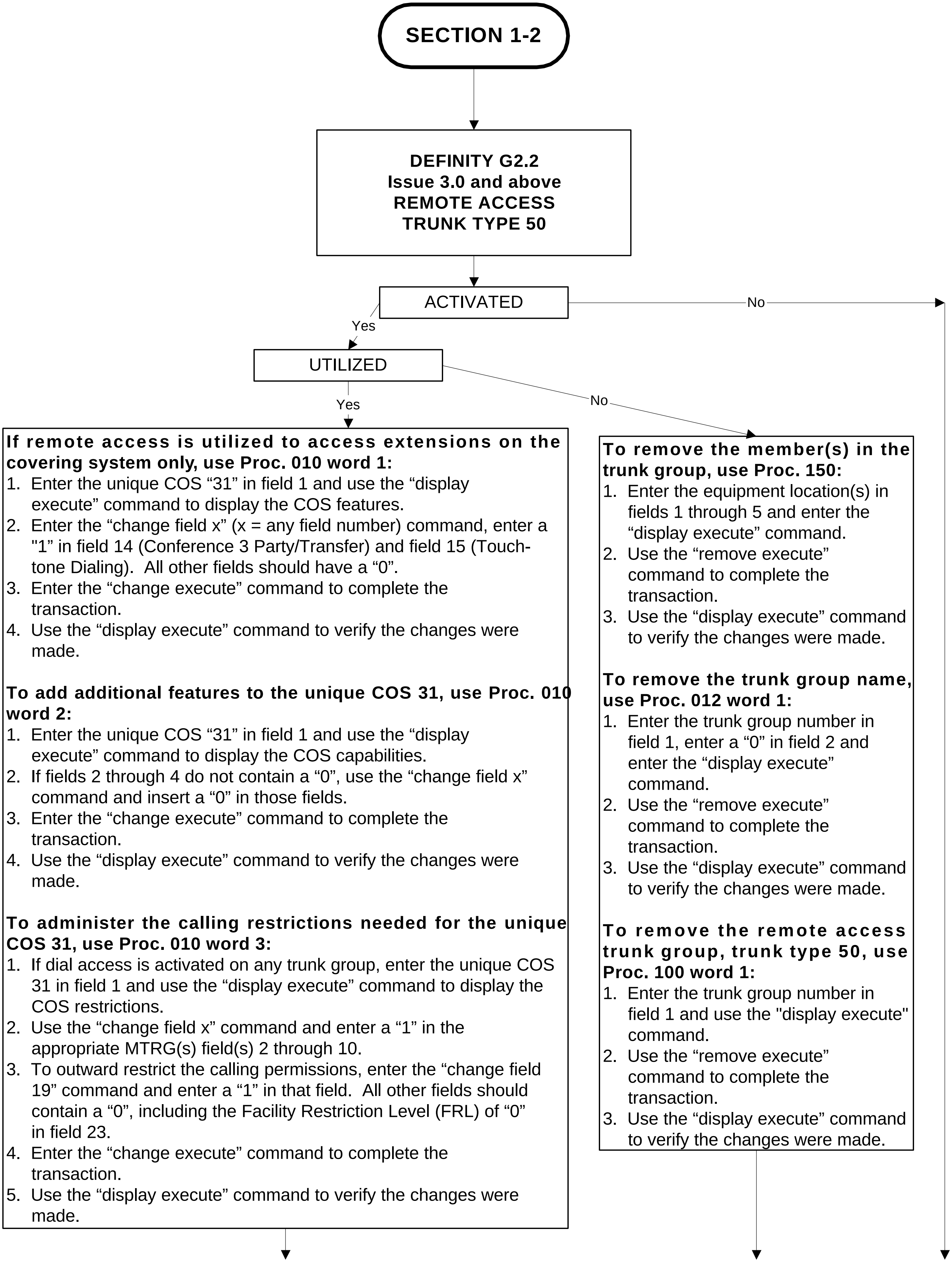
To remove the remote access trunk group, trunk type 50, use Proc. 100 word 1:

1. Enter the trunk group number in field 1 and use the “display execute” command.
2. Use the “remove execute” command to complete the transaction.
3. Use the “display execute” command to verify the changes were made.

In the software issues of R2V4N or G2.2 issue 3.0 and above, you have the ability to permanently disable the remote access feature, use Proc. 275 word 4:

1. Use the “display execute” command to display features and arrangements associated with the system.
2. Use the “change field 2” command and enter a “1” in that field.
3. Use the “change execute” command to complete the transaction.
4. Use the “display execute” command to verify the changes were made.

NOTE: Always write the new translations to the tape in the system when changes are complete by using the “run tape execute” command.



SECTION 1-2

DEFINITY G2.2
Issue 3.0 and above
REMOTE ACCESS
TRUNK TYPE 50

ACTIVATED

No

Yes

UTILIZED

Yes

No

If remote access is utilized to access extensions on the covering system only, use Proc. 010 word 1:

1. Enter the unique COS “31” in field 1 and use the “display execute” command to display the COS features.
2. Enter the “change field x” (x = any field number) command, enter a "1” in field 14 (Conference 3 Party/Transfer) and field 15 (Touch-tone Dialing). All other fields should have a “0”.
3. Enter the “change execute” command to complete the transaction.
4. Use the “display execute” command to verify the changes were made.

To add additional features to the unique COS 31, use Proc. 010 word 2:

1. Enter the unique COS “31” in field 1 and use the “display execute” command to display the COS capabilities.
2. If fields 2 through 4 do not contain a “0”, use the “change field x” command and insert a “0” in those fields.
3. Enter the “change execute” command to complete the transaction.
4. Use the “display execute” command to verify the changes were made.

To administer the calling restrictions needed for the unique COS 31, use Proc. 010 word 3:

1. If dial access is activated on any trunk group, enter the unique COS 31 in field 1 and use the “display execute” command to display the COS restrictions.
2. Use the “change field x” command and enter a “1” in the appropriate MTRG(s) field(s) 2 through 10.
3. To outward restrict the calling permissions, enter the “change field 19” command and enter a “1” in that field. All other fields should contain a “0”, including the Facility Restriction Level (FRL) of “0” in field 23.
4. Enter the “change execute” command to complete the transaction.
5. Use the “display execute” command to verify the changes were made.

To remove the member(s) in the trunk group, use Proc. 150:

1. Enter the equipment location(s) in fields 1 through 5 and enter the “display execute” command.
2. Use the “remove execute” command to complete the transaction.
3. Use the “display execute” command to verify the changes were made.

To remove the trunk group name, use Proc. 012 word 1:

1. Enter the trunk group number in field 1, enter a “0” in field 2 and enter the “display execute” command.
2. Use the “remove execute” command to complete the transaction.
3. Use the “display execute” command to verify the changes were made.

To remove the remote access trunk group, trunk type 50, use Proc. 100 word 1:

1. Enter the trunk group number in field 1 and use the "display execute" command.
2. Use the “remove execute” command to complete the transaction.
3. Use the “display execute” command to verify the changes were made.

You have the ability to permanently disable the remote access feature. Use Proc. 275 word 4.

1. Use the “change field 2” command and enter a “1” in that field.
2. Use the “change execute” command to complete the transaction.
3. Use the “display execute” command to verify the changes were made.

NOTE: Always write the new translations to the tape in the system when changes are complete by using the “run tape execute” command.

If remote access is utilized to access the public switch netwok, assign the maximum length Barrier Code (only one 4 digit barrier code can be assigned per system.) and Authorization Codes (assign a unique 7 digit authorization code per user). Do not assign these codes in sequential order or the same numbers, (i.e. 1234, 6543, 1111, 9999).

The 4 digit Remote Access Barrier Code is assigned via the console using a feature access code. To find the feature access code, use Proc. 350 word 2:

1. Enter a “26” (Remote Access-change barrier code) in field 1 and use the “display execute” command to display the feature code.

To program the 4 digit barrier code from the console:

1. At the console depress the “loop” key then the “start” key to get dial tone.
2. Dial the feature access code that was displayed in Proc. 350 word 2 and the 4 digit barrier code you want to assign. When confirmation tone (3 beeps) is heard, press the “release” key on the console to complete the transaction.

To administer the network trunk group parameters and authorization code requirements for incoming remote access trunk groups, use Proc. 103 word 1:

1. Enter the remote access trunk group number in field 1. Use the “display execute” command to display the trunk group parameters.
2. Enter the “change field 2” command and enter the appropriate Facility Restriction Level (FRL) in that field.
3. Enter the “change field 6“ command and enter a “1” in that field.
4. Use the “change execute” command to complete the transaction.
5. Use the “display execute” command to verify the changes were made.

To assign the 7 digit authorization code, use Proc. 281 word 1:

1. Enter a “7” in field 1. Use the “change execute” command to complete the transaction.
2. Use the “display execute” command to verify the changes were made.

To assign the (FRL), Network Access Flag and Extension Partition associated with a single authorization code, use Proc. 282 word 1:

1. Enter the 7 digit authorization code you wish to assign in field 1.
2. Enter the appropriate FRL to allow the remote access call in field 2.
3. Enter the appropriate Network Access Flag, a “0”(on-net access to off-net users not allowed) or “1” (on-net access to off-net users allowed).
4. Enter the Extension Partition if applicable in field 4.
5. Use the “add execute” command to complete the transaction.
6. Use the “display execute” command to verify the changes were made.

To administer the barrier code and authorization code requirements for access to AAR/ARS, use Proc. 285 word 1:

1. Use the “display execute” command to display the system class of service (COS) features and capabilities for the network.
2. Enter a “4” (barrier code and authorization code required) or “5” (barrier code and authorization code required with no prompt for authorization code) in field 1.
3. Use the “change execute” command to complete the transaction.
4. Use the “display execute” command to verify the changes were made.

To administer the features needed for the unique COS 31 use Proc. 010 word 1:

1. Enter the unique COS “31” in field 1 and use the “display execute” command to display the COS features.
2. Enter the “change field x” (x = any field number) command. Enter a “1” in field 14 (Conference 3 Party/Transfer) and field 15 (Touch-tone Dialing). All other fields should have a “0”.
3. Enter the “change execute” command to complete the transaction.
4. Use the “display execute” command to verify the changes were made.

To add additional features to the unique COS 31, use Proc. 010 word 2:

1. Enter the same unique COS “31” in field 1 and use the “display execute” command to display the COS capabilities.
2. If fields 2 through 4 do not contain a “0”, use the “change field x” command and insert a “0” in those fields.
3. Enter the “change execute” command to complete the transaction.
4. Use the “display execute” command to verify the changes were made.

To administer the calling restrictions needed for the unique COS 31, use Proc. 010 word 3:

1. If dial access is activated on any trunk group, enter the unique COS “31” in field 1 and use the “display execute” command to display the COS restrictions.
2. Use the “change field x” command and enter a “1” in the appropriate MTRG(s) field(s) 2 through 10. To restrict the appropriate calling permissions, enter the “change field x” command and place a “1” in fields 11 through 22 to activate the appropriate restriction. Enter the “change field 23” command and enter the lowest Facility Restriction Level (FRL) in that field to complete the outgoing call.
3. Enter the “change execute” command to complete the transaction.
4. Use the “display execute” command to verify the changes were made.

NOTE: Always write the new translations to the tape in the system when changes are complete by using the “run tape execute” command.

END