GENERAL DESCRIPTION - PROTECTION OF TEST LINE NUMBERS FROM UNAUTHORIZED USE

1. GENERAL

1.001 This Addendum is issued to restrict access to Division 302 of the Bell System Practices and all company test number directories containing this information.

1.002 Transmission test lines, especially the loop around have provided a means for defrauding the Company. It is essential these test line numbers be treated as private company proprietary information and that they not be revealed in any way to unauthorized persons.

1.003 Loop around test lines must be equipped to provide "off-hook" supervision. It is also desirable that such equipment be equipped with a standard option that prevents "talk through" by unauthorized persons. If the loop around equipment is not protected by these options, recommendations should be forwarded to the Chief Engineer for their modification.

2. PROTECTION OF TRANSMISSION TESTING DIRECTORIES

2.01 All company directories listing test numbers must be noted in bold letters in a conspicious location on each sheet with the following: "COMPANY PRIVATE" or "BELL SYSTEM PROPRIETARY INFORMATION. NOT FOR PUBLICATION OR OUTSIDE DISTRIBUTION."

2.02 Ordinarily, these test line directories must be stored in a locked desk, drawer, file, etc. During normal working hours the directories may be made more convenient, however, they should not be exposed to unauthorized persons. Most test numbers are listed in the 302 division of the Bell System Practices. However, there may be lists prepared locally and these too should be protected as described herein. Where the Bell System Practices are stored in open files, the 302 Division should be removed and a note should be placed in the sequential position of 302-XXX-100 describing where the practice may be obtained.

2.03 Out of date or replaced test line directories must be destroyed by mutilation or other equally effective means, they are not to be discarded intact in wastebaskets.

3. REPORTING UNAUTHORIZED USE OF TEST NUMBERS

3.01 Test numbers suspected of being misused should be reported promptly through organizational channels to the Security Manager or Security Supervisor.