SYSTEM PROTECTION AND PHYSICAL SECURITY REQUIREMENTS
MINICOMPUTER MAINTENANCE AND OPERATIONS CENTER
COMPUTER SYSTEM MEASUREMENT
INFORMATION SYSTEMS

CONTENTS PAGE

Figure

1. GENERAL

1.01 This section discusses the importance of minicomputer system protection and security for Operations Support Systems (OSSs) located in the Minicomputer Maintenance and Operations Center (MMOC). Suggestions are given for the design of the physical plant, safe operating procedures, prevention of data loss, and for protection against deliberate damage. Section 190-020-553, Issue 1 is being renumbered with the release of this document.

1.02 Whenever this section is reissued, the reason for reissue will be listed in this paragraph.

1.03 The title of each figure includes a number(s) in parentheses which identifies the paragraph(s) in which the figure is referenced.

1.04 The use of General Trade Products (GTP) vendor's terms or procedures does not imply endorsement or exclusion of other products. For brevity and simplicity, only products which are presently a significant factor in OSS design and support are covered. Other products may be included at a later date.

2. BUILDING CONSIDERATIONS

Computer Room Planning

2.01 The functions performed by OSSs and other data processing systems located within a Minicomputer Maintenance and Operations Center are essential to the conduct of company operations and the maintenance of telephone plant. Any of the following can cause the loss of data processing capability and seriously affect service:

- Storms, floods, and other natural disasters
- Loss of commercial AC power or air-conditioning failures

- Fires
- Accidents
- Carelessness or deliberate damage.

2.02 In designing and engineering a computer center for OSSs, companies should consider the relative importance of the systems that may be installed and the cost penalties that may ensue if system protection and reliability requirements are not given careful consideration at this time.

2.03 Computer room planning should be a joint departmental effort which includes representation of the Minicomputer Support Group (MSG), Building Engineering, Data Systems, and MMOC maintenance and operations personnel to ensure that space, environmental, and communications needs are met.

Site Preparation

2.04 This section is not intended to provide detailed information on building and room construction details for OSSs. Sections 007-590-200 and 007-590-301 through 007-590-305 discuss computer center physical security and disaster recovery. These sections contain a complete list of guidelines to be followed. A general indication of the considerations for site preparation, security, and disaster recovery are also contained in these sections.

2.05 Recommendations for building planning may be found in Section 760-250-150, Building Planning for Electronic Data Processing Systems, and in Section 760-150-155, Building Planning for Operations Support Systems. Guidelines for protective AC power for OSSs are provided in AT&T General Letter (GL) 77-04-087; similar guidelines for Data Processing Centers may be found in GL 77-08-178. Other sources that should be consulted are:

(a) Site preparation guidelines furnished by the various computer system manufacturers.

(b) National Fire Protection Association (NFPA) Recommended Standards

- Standard for the Protection of Electronic Data Processing Equipment (NFPA 75)
- National Electrical Code (NFPA 790)

(c) National and local building codes

(d) Occupational Safety and Health Act (OSHA)

(e) Bell System Practices for Fire and Safety.

Building Planning

2.06 Consult the reference material mentioned in paragraph 2.05 for recommendations to be followed in planning the computer center. MMOC planning should include the following considerations:

(a) Fire resistant construction methods and techniques to be employed.

(b) The number of access points and their security. A minimum of two doors must always be provided. The second (or emergency exit) door should be equipped with panic hardware.

(c) Emergency lighting in the event of power or lighting circuit failure.

(d) Use of viewing windows is ***not*** recommended because this violates the integrity of the one hour fire rated enclosure and MMOC security requirements.

(e) Provision of a master disconnect switch as a part of the main service wiring controlled from a location readily accessible at the main control panel and at the principal exit doors. This master power control, when actuated, should disconnect the power to all of the equipment in the MMOC and to the air-conditioning system serving the area. This switch should be clearly marked and guarded to preclude use in all but emergency conditions affecting the entire cluster.

(f) Provision of temperature and humidity recording instruments.

(g) Provision of audible and visual environmental alarms.

(h) Extension of environmental alarms to a remote location providing 24-hour coverage.

2.07 If construction work is necessary to build the computer room, provide sufficient time for the environment to stabilize (eg, dust through filtration, dampness from new concrete, etc) before installing the computer hardware.

3. POWER REQUIRMENTS

3.01 Computer installations require a high quality, reliable commercial AC power source. To determine the quality of the power that would be supplied to a particular installation, a power line monitoring program should be undertaken to record line disturbances over a period of several months so that the data recorded would include seasonal disturbances as discussed in GL 77-04-087/EL 5223. This GL provides details on a recommended method of evaluating the need as well as determining the cost effectiveness of the various forms of AC protection that might be considered for each installation. Minicomputer systems may "crash" if the AC power variation tolerances are exceeded. In areas where AC power fluctuations exceed the manufacturer's tolerances, the installation of an uninterruptible power supply (UPS) should be considered for essential systems if it can be economically justified. Part VII of Engineering Letter (EL) 5223 contains recommendations on technical and economic studies that should be considered in determining the need for AC protection. Recommended Letter (RL) 79-10-034 contains additional guidance on provision of protected AC power for OSSs.

3.02 High voltage commerical service should be distributed directly to a dedicated step down transformer located in the vicinity of the OSS installation. If this is not possible, provide a dedicated feeder from the local distribution board. In locations equipped with standby power (ie, engine alternators), the dedicated feeder should be provided as a "special" AC service bus. This means that the feeder will permit the OSS to operate on commerical power while the engine-alternators are being routined. Switchgear should be provided to enable this feeder to be powered from the engine-alternator during periods when commerical power may not be available.

3.03 If all or some of the systems located in the MMOC must continue to operate after the primary power source has failed, provide an emergency engine alternator with sufficient capacity to provide for the computer systems, essential room lighting and air/chilled water conditioning of the equipment areas. Without air-conditioning, heat can build up rapidly within a minicomputer system. If not shut down manually by operating personnel, the minicomputer systems will exceed design temperature limits and "crash". This is likely to cause component damage that may become evident either at the time of system restoral or later due to shortened component life because of the resultant heat stress.

3.04 Follow proper grounding practices to protect operating personnel and prevent erratic system operation. Consult system ELs, Section 802-001-193, Section 802-001-198, and vendor installation manuals for specific grounding instructions.

4. OSS PROTECTION AND SECURITY

4.01 A comprehensive security program should be prepared and implemented at each MMOC. An effective plan must include preventive measures and controls designed to prevent accidental or deliberate damage, destruction or misuse of OSS and other on-line computer systems, their software, data files or supplies. The objectives of the security program are:

(1) To safeguard employees from physical harm.

(2) To protect the property of the company from loss or damage that would interrupt or seriously impair data processing activities.

(3) To provide reasonable assurance that the company can carry on essential OSS functions if normal MMOC activities are disrupted.

Prevention

4.02 Control access to the computer room and associated high risk security areas in the following manner.

(1) Restrict access to the computer operations center to a single point. Equip the emergency exit with alarm features to alert operations or security personnel whenever the door is opened. Preferably, access should be via the administrative area.

(2) Control access by the use of magnetically coded door locks, magnetic badge readers, electric locks, or other approved procedures. Provide master keys and equip automatic locking doors with fail safe locks in the case of a power failure.

(3) Maintain an up-to-date, authorized access list. Change magnetic code or lock combinations

immediately if a card or other entry device is in the possession of an individual who is not authorized to enter the area.

(4) Control access to sensitive areas by unauthorized persons including other telephone company employees. Building or contractor services should be performed during normal MMOC working hours whenever possible. An MMOC representative must be present at all times when any such work is to be done at a time when the MMOC is normally unattended. Each MMOC should maintain a visitor's log. Visitors should be required to log in and out, and wear a visitor's badge at all times. MMOC employees who may be assigned to work in the MMOC at a time when it is normally unattended should be required to sign in and out for their own protection. Institute controls to ensure that all log entries are complete and that all visitor's badges are accounted for.

(5) Do not advertise computer center locations. Avoid all unnecessary references in company publications and in public relations distributions. Do not include OSS computer centers in guided tours open to the general public.

5. DETECTION

5.01 Provision should be made for a means of detecting any unauthorized entry into sensitive areas outside of normal working hours. Items for consideration include:

(a) Main door alarms that are activated out of hours.

(b) Intrusion alarms such as motion detectors.

(c) Closed circuit television monitoring and/or video tape recording.

6. SAFEGUARDING ESSENTIAL RECORDS

6.01 Essential records such as OSS data bases and other data that would be difficult or impossible to recover following the loss of or damage to the originals must be duplicated and stored in a secure area at another location. Storage of these backup records in the same building is unacceptable unless access can be assured and the danger of loss or damage is eliminated.

6.02 The storage area must meet the same environmental standards discussed in Section 190-020-551.

6.03 Equip the alternate storage area with a lockable data safe. The safe selected should meet the minimum requirement of the Underwriter's Laboratories Fire Class 150 Two-Hour Label.

6.04 Follow recommended procedures for the preparation of backup copies of essential information.

6.05 Establish controls over the movement of backup records to and from the alternate storage site and institute a check procedure at each location to acknowledge receipt of the records.

7. BOMB THREATS

7.01 MMOC management is responsible for ensuring that all operations personnel are familiar with company procedures and guidelines for handling bomb threats. These should be reviewed with all employees periodically. A copy should be readily available in the MMOC administrative area.

8. OTHER SECURITY SAFEGUARDS

8.01 Other security items that must be considered are the security of other building areas that provide essential services to the MMOC.

(a) Power and air-conditioning rooms and circuit breaker cabinets must be locked. Consideration should be given to keying critical equipment rooms differently.

(b) Lock any telephone closet located outside of the MMOC where cross-connections are made to house cable.

8.02 Provide route or sheath diversity in Outside Plant facilities connecting the MMOC to the nearest central office location.

8.03 No device should be allowed in the computer room or media library that is capable of generating a high intensity magnetic field. Minicomputer systems and magnetic media containing programs and other data must not be exposed to magnetic fields with intensities that exceed 0.5 V/M in the frequency range 10kHz to 1gHz.

8.04 Any device such as a walkie-talkie or a CB radio that may be a source of Radio Frequency Interference (RFI) should not be used close to operating minicomputer systems. Radio frequency electric fields of a field strength greater than 1 to 2 volts per meter can cause OSS failures. Check to see if RF shielding from outside sources is necessary. Section 760-220-110, RFI Shielding, discusses the procedure to detect and (if necessary) shield against radio interference. Signs prohibiting the use of transmitters should be posted conspicuously in the MMOC (see Fig. 1).

9. ALARMS

9.01 A comprehensive alarm system for the MMOC and associated high security area should be installed. The alarm system should include the following items:

(a) Operation of the early warning fire detection system

(b) Opening of main door (after hours)

(c) Opening of emergency exit door

(d) Failure of commerical AC power

(e) Failure of air-conditioning system

(f) Failure of flow of liquid coolant

(g) Temperature and humidity alarms.

9.02 The air-conditioning and liquid coolant alarm should provide a two-stage temperature warning prior to shut-down.

9.03 Alarms should be installed in an attended part of the building such as the guardroom or an attended maintenance area. Provide alarm transfer features or alarm multiples so that MMOC alarms can be monitored at a constantly attended location during periods when the MMOC is unattended. The use of a computer based alarm surveillance system to monitor alarm status may also be considered.

9.04 Each remote monitoring location should be provided with emergency call-out lists and procedures in accordance with company instructions. Review and update these lists periodically to ensure their accuracy. This list should contain the name and contact number of a duty supervisor depending on company policy.

9.05 Alarms and alarm multiples or alarm transfer features should be tested at prescribed intervals so that they will function if an emergency occurs.

10. FIRE PROTECTION

Storage of Combustibles

10.01 Computer center operations may require considerable quantities of paper stock and other combustible supplies. Since the material presents a considerable fire hazard, the quantity of paper, spare magnetic tapes or any other combustible items that may be in the computer room should be kept to an absolute minimum. Until needed, store this material in enclosed metal file cases or in fire resistant containers.

10.02 Store computer supplies in an external storage area until needed. Recording media should be stored in a media storage or tape library.

10.03 Dispose of waste paper at frequent intervals. Maintain good housekeeping practices at all times to prevent the accumulation of any combustible material in the computer room area.

10.04 Smoking in the computer room area or in the media storage library should not be allowed. Post ***"NO SMOKING"*** signs at conspicuous locations in these areas. If possible, provide authorized smoking areas for employees.

Fire Detection Systems

10.05 An approved early warning fire detection system should be installed throughout the computer room within concealed floors and ceilings, the media library and adjacent storage and administrative areas. Make sure the system will function during a loss of normal AC power.

10.06 The fire detection system must provide audible and visual alarms within the computer operations area and to other areas of the building such as a guard area or an attended maintenance area. Transfer features that will transfer alarms to an attended location at times when the MMOC may be unattended should be included.

11. FIRE PROTECTION EQUIPMENT

11.01 Use a master fire extinguishing system of the type that uses hydrocarbon bromide (Halon) as an extiguishing agent. A system of this type will reduce equipment damage to a minimum while presenting little hazard to personnel.

11.02 Nonwetting fire extiguishing agents for electrical equipment should be carbon dioxide or Halon fire extinguishers (Section 760-660-150). Water type extinguishers should be provided to protect against fires in ordinary combustible materials such as paper. One fire extinguishing station containing both types should be provided for every 6000 square feet, taking into account the maximum travel distance of 75 feet.

11.03 At least two floor lifters should be mounted at conspicuous locations in the computer room. Clearly mark them for fire emergency use.

11.04 Prominently display the fire department telephone number near telephones in the computer room, media library and the administrative area.

12. FIRE EMERGENCY PLANNING

12.01 Each Minicomputer Maintenance and Operations Center must prepare a detailed Fire Emergency Plan to ensure that all employees working in the MMOC are fully aware of their duties and responsibilities in the event of a fire alarm or fire emergency condition. The employees should receive on-going training to ensure that they can perform these duties successfully.

12.02 MMOC personnel who may be expected or assigned to use portable fire extinguishers should receive training in the use of carbon dioxide or Halon fire extinguishers. All personnel must be cautioned not to use water type extinguishers on fires in the computer systems or on any electrical equipment.

12.03 A typical Fire Emergency Plan would include procedures and assignments such as the following:

(a) Investigate the fire alarm.

(b) In case of fire, call the Fire Department. Give the building address and room number. Inform the Fire Department that the fire involves a computer center and that toxic gasses may be produced by burning recording tapes.

(c) Evacuate nonessential personnel.

(d) Turn off the air-conditioning system.

(e) Atempt to contain the fire.

(f) Power down the computer systems. If time and conditions permit, power down each system individually according to standard instructions.

(g) ***In an emergency situation, operate the master power disconnect switch.***

(h) Wait outside of the building to act as a guide for the Fire Department.

13. FIRE AND SAFETY INSPECTION

13.01 M & M Protection Consultant, a service of Marsh & McLennan, will furnish advice with respect to fire protection and safety in the case of new construction and important alterations. M & M will also provide scheduled, detailed inspections of data processing installations that appear on a prepared list for protection submitted by a TELCO. Section 760-650-150 provides a general outline of the fire and safety inspection and advisory service provided by M & M Protection Consultants.

13.02 Each MMOC must conduct periodic fire and safety inspections as specified by company instructions.

13.03 Fire emergency plans should include an invitation to the local Fire Department to inspect areas and make them aware of the equipment location, access, etc.

14. CONTINGENCY PLANNING

14.01 In spite of all precautions, disruptions of normal data processing services can and will occur in a MMOC. These service failures may be relatively minor such as an intermittent hardware of software problem that affects only one system, or may be more serious such as a commerical power or air-conditioning failure that will affect all MMOC systems until the problem is corrected.

14.02 Companies should prepare contingency plans for the restoration of essential OSS service. Such a plan may be relatively simple, such as a procedure for escalating a trouble report within the TELCO or vendor organizations after a specified time has passed without a trouble clearance. Other plans will be much more complex. A contingency plan should:

(1) Identify essential OSSs

(2) Identify systems or functions that can be backed up manually

(3) Determine service restoration priorities

(4) Detail restoration procedures

(5) Identify available resources.

Detailed contingency planning procedures for computer centers are contained in Section 007-590-304.

14.03 Some examples of procedures for maintaining essential service are as follows.

(a) ***Load Shedding:*** Shutting down nonessential systems to relieve the power or air-conditioning load during a crisis situation. In extreme cases, one unit of a duplex or triplex configuration could be shut down if the configuration is such that service will not be impaired.

(b) ***Service Rearrangements:*** Moving priority services from an OSS experiencing trouble to another system which may be a "hot spare" or alternate active system. If the alternate system does not have any unused capacity, this will entail the denial of service to some users. Since this may require extensive effort, it should only be considered in situations where long outage times are anticipated.

(c) ***Emergency AC Power:*** Obtaining a transportable engine/alternator for emergency use during a commerical power failure if a standby engine/alternator has failed or has not been provided.

Caution: Before using any such equipment, ensure that voltage phasing and cycling falls within specified limits under load.

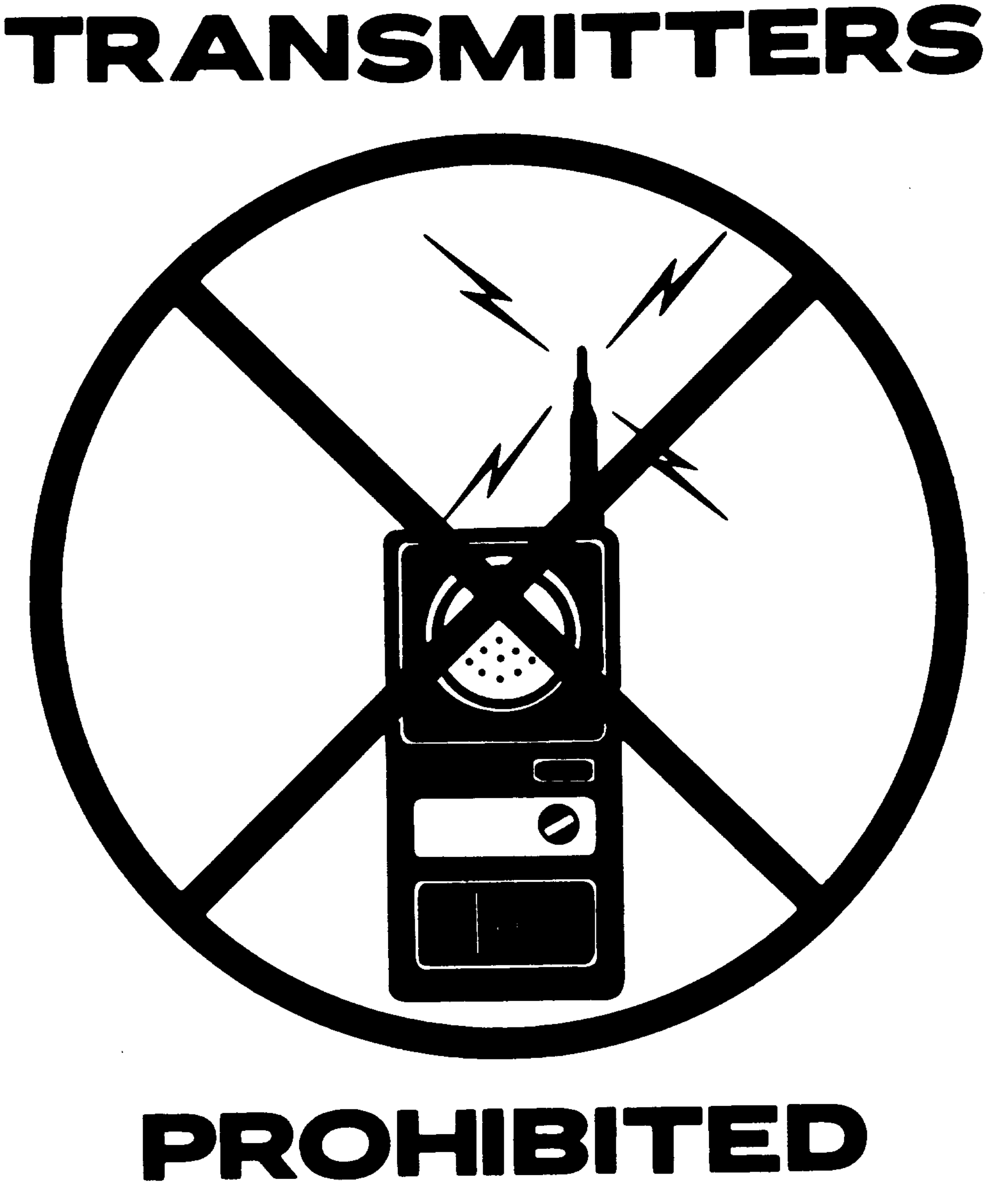

Fig. 1—Transmitter Warning Sign (8.04)