SSGT FEENSTER 5114

DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
WASHINGTON, D.C. 20380

MCO P5510.14 w/CH 1
CCIR-40:sbe
2 Jan 1981

MARINE CORPS ORDER P5510.14

From: Commandant of the Marine Corps
To: Distribution List

Subj: Marine Corps Automatic Data Processing (ADP) Security Manual

Ref: (a) OPNAVINST ~~5510.1F~~ 5239.1A
(b) MCO P5600.31E
(c) MCO 5600.45A

Encl: (1) LOCATOR SHEET

1. Purpose. To publish the technical direction and guidance governing the security of Marine Corps ADP activities.

2. Background. The policies contained in this Manual have been developed in accordance with reference (a) to provide, at field ADP activities, the guidance necessary for the uniform and effective safeguarding of classified and sensitive information.

3. Action. Upon receipt, commanders with organizational control of ADP activities will implement the provisions of this Manual.

4. Distribution. This Manual has been assigned Distribution Code A55, and those activities concerned will receive updated printouts of their Individual Activity Table of Allowances for Publications indicating Distribution Code A55. Requests for increase or decrease in allowance quantities should be submitted to the Commandant of the Marine Corps (Code HQSP) in accordance with reference (b). A future change to reference (c) will include Distribution Code A55.

5. Recommendations. Recommendations concerning the contents of the Marine Corps Automatic Data Processing (ADP) Security Manual are invited. Such recommendations should be forwarded to the Commandant of the Marine Corps (Code CCIR) via the appropriate chain of command.

6. Reserve Applicability. This Manual is applicable to the Marine Corps Reserve.

7. Certification. Reviewed and approved this date.

Robert R Hull

ROBERT R. HULL
By direction

DISTRIBUTION: A55 plus 7000067 (50)

Copy to: 8145001

PCN 102 084902 00

3. Protection of Other Remote Access or Data Entry Equipment. Physical security safeguards for other remote access devices and the areas which house them will be determined on a case-by-case basis by the using component and the cognizant supporting security element.

3011. SECURITY REVIEWS. Physical security reviews of computer facilities and alternate facilities designated as critically sensitive will be conducted annually as part of the facility risk management program (see chapter 10). Specific items for consideration should include adequacy of physical protection, access/egress control and use of guard personnel from the first barrier (wall) surrounding the computer system outward. Contingency plans for breaches of physical security, bomb threats, fire, and natural disaster will also be assessed. Internal operating procedures and computer system security will not be inspected by physical security inspectors.

3012. ENVIRONMENTAL SECURITY. The protection of sensitive computer facilities from the effects of fire, flood, wind, and other natural phenomenon is an important element of any comprehensive, cost-effective physical security program. It is recognized that some computer installations require a higher level of environmental protection than others. Such factors as the monetary value of the equipment, operational requirements for uninterrupted system availability, local site considerations, and the uniqueness and resulting difficulty in replacing system components will influence the amount of resources committed to ensure that an adequate level of environmental security has been provided. This section will primarily prescribe protective measures for fire and water damage as it is presumed that the need to provide adequate protection against wind, earthquake, and naturally caused flooding was considered during the site selection and computer room construction phases of physical security planning.

1. Fire Protection Codes and Standards. Adequate fire protection for essential ADP systems is achieved through a combination of minimizing the exposure to fire damage by ensuring prompt detection, and by providing adequate means to extinguish the fire. In general, Marine Corps ADP activities will conform to the standards contained in the National Fire Code, Volume 7, specifically the National Fire Protection Association (NFPA) Code No. 75, "Standard for the Protection of Electronic Computer/Data Processing Equipment"; NFPA 72, "Automatic Fire Detectors"; NFPA 80, "Fire Doors and Windows"; and NFPA 70, "National Electrical Code."

2. Computer Room Fire Prevention. Fire prevention is heavily dependent upon the physical characteristics of the area housing the equipment. Experience has shown that fires are more likely to start in adjacent offices or rooms (rather than in the facility itself), and then spread to the data processing area. Thus, these areas should also be considered when planning a comprehensive fire protection system. The current edition of MCO P11000.11 outlines fire prevention and protection requirements.

a. Operational Practices. Within the facility, good housekeeping and safe operating procedures are prerequisites to maintaining a safe environment. Lint from moving paper and cards ignites very easily and burns rapidly. The space under raised floors collects lint and should be cleaned regularly. Paper stocks, other than small quantities for immediate use, will not be stored in the main computer room or in auxiliary ADP equipment rooms.

b. Facility Construction. All materials used in the construction of computer rooms or related facilities, to include those composing walls, floors, partitions, finish, acoustical treatment, raised floors, raised floor support, and suspended ceiling, will have a National Fire Protection Association (NFPA) flame-spread rating of 25 or less (see NFPA No. 255-1972, Method of Test of Surface Burning Characteristics of Building Materials).

c. Power-Off Controls. The power-off controls for the electrical system shall disconnect the air-conditioning system serving the computer equipment room and the power to all electric equipment in the room, except lighting. Disconnecting devices will be placed at locations readily accessible to operating personnel, preferably at designated exit doors. These will be covered to prevent inadvertent or accidential operation. Procedures will be established to ensure the cables are properly connected.

d. Smoke Exhaust. Computer equipment rooms should be equipped with a smoke exhaust capability to minimize possible hazard to personnel, equipment, and storage media. Air-conditioning systems at all Marine Corps computer equipment rooms should be equipped with dampers to prevent the spread of fire, smoke, and chemical agents.

3. Computer Room Fire Detection Systems. Experience has shown repeatedly that prompt detection is a major factor in minimizing fire damage to ADP facilities. Facilities housing essential ADP equipment will be equipped with fire detection equipment which detects the byproducts of combustion. Consideration should also be given to locating detection sensors in rooms or areas adjacent, above or below a computer equipment room where a significant danger of fire exists. While each detection system installation should be specifically engineered, the following are the desirable characteristics that a detection system should possess.

a. Detectors should be located so as to detect equipment fires as early as possible.

b. The detection system should be capable of indicating the area of the room where the potential fire exists. This will permit rapid inspection of the area by computer room personnel before further unnecessary and/or expensive action is initiated.

c. An alarm should be connected to a monitor panel within the center and, possibly, at a continuously manned guard or fire station, particularly, if the facility is sometimes unmanned.

d. Alarm systems, particularly those which are designed to activate quenching systems, should be equipped with a delay feature that will permit inspection of the possible trouble area and evacuation of the room before extinguishing agents are released.

e. The fire detection system should be designed and installed so that it cannot be easily deactivated, either maliciously or accidentally.

4. Computer Room Fire Extinguishing Measures. The type of fire extinguishing equipment utilized will vary in accordance with the physical characteristics of the facility, the mission of the computer system, and the monetary value of the equipment. A minimum degree of fire protection provided primarily by hand-held extinguishing equipment will be implemented with additional protection provided by an area extinguishing system, as appropriate.

a. Portable Firefighting Equipment. The provisions of this paragraph are designed to ensure that fire extinguishing equipment will be immediately available for use in controlling fires in a computer equipment area. A carbon dioxide or halon fire extinguisher of at least 15-pound capacity will be available for use on electrical fires. Water-type fire extinguishers will also be available for use on nonelectrical fires. Extinguishers will not be located further than 50 feet from any piece of computer equipment. The location of the extinguishers should be indicated through the use of clearly recognizable signs posted high enough on the wall over the extinguisher so as to be visible from any point in the room. Suction devices for removing raised floor panels shall be available at each extinguisher location, if appropriate. Hand-held extinguishing equipment shall be marked to indicate the type of fire for which

it is intended. Periodic training (not less than once annually) should be given to computer personnel on the operation of all extinguishing equipment installed at each ADP activity.

b. Area Extinguishing Systems. The primary agents used in area extinguishing systems are water, carbon dioxide (CO2) and halon. CO2 systems, water sprinkler systems and halon volumetric, deluge systems have relative advantages and disadvantages that must be weighed against such variables as cost, computer room construction characteristics, and operational recovery requirements, etc.

c. Fire Drills and Other Related Training. Facility managers will ensure that orientation and training classes are held periodically to enable personnel who work in or around a computer equipment room to become familiar with facility fire emergency equipment and procedures.

5. Fire Protection of Data Storage Areas. Because data storage media will sustain combustion, they represent a different type of fire hazard. Another consideration is that magnetic tapes, tape reels, and disk pack containers become distorted and unusable at temperatures above 150 degrees fahrenheit (66 degrees Centigrade). Because of this greater sensitivity to heat, the walls, floors, and ceilings of a storage area should have a 2-hour fire rating. The most commonly used means of protecting storage media is by a water sprinkler system. The temperature setting of the heads initiates operation before any major damage is done to storage media. When this type of extinguishing system is used, sufficient drains must be placed in the floor to prevent unnecessary water collection in the affected area. Halon systems are equally suitable for use in data storage areas. An appropriate number of portable fire extinguishers should also be placed in these areas.

6. Protection of Computer Supplies. Computer supplies are the most combustible material used in a data processing installation. Consequently, the ideal solution to the danger posed by these paper stocks is to store as few as possible in the computer facility itself. A central storage location which is as fire resistant as practical should be utilized. This area can be equipped with suitable fire alarms and extinguishing systems, if deemed appropriate, after such factors as value, criticality to operation, and proximity to central computer complex are considered.

7. Local Fire or Police Assistance. The director of each ADP activity should ensure that adequate procedures have been established to obtain firefighting assistance from the appropriate local fire departments. This should include provisions for adequate alarm and communication procedures, and assuring that computer personnel are familiar with fire contingency plans and necessary actions in the event of fire. Consistent with good security practice, local fire department officials should be invited to visit the facility, review the fire protection system being utilized, and discuss with appropriate personnel matters involving fire protection of the computer facility. In most cases, both the need for good security and local fire protection can be satisfied by careful planning and coordination. Local law enforcement agencies should also be contacted to review plans for providing support in the event of civil emergencies or other problems at the facility which might affect essential data processing activities.

8. Protection Against Water Damage. Below ground or basement sites are particularly vulnerable to flooding from backed up sewer lines, broken water mains, heavy rain, and swollen streams. If such a site is utilized, provisions should be made for drains, pumps and emergency power for pumps. No matter where the computer installation is located, a fire on the floor above will result in excessive buildup of weight and water that will probably produce leakage into the facility. The use of drains, bunkers, and channels, consistent with security requirements, will alleviate potential problems of this nature. Floor-to-floor integrity designed into buildings is often lost by drilling holes for

utilities. These holes should be sealed to prevent their use as a path for fire or water. An additional protection against water damage is the use of plastic sheeting to cover vital pieces of equipment. As previously discussed, equipment must be deenergized when water or high humidity are present. Plastic covers should be removed promptly when no longer required so as to prevent excessive heat buildup.

3013. PROTECTION OF SUPPORTING UTILITIES. Every ADP facility is dependent upon supporting utilities: electric power, air-conditioning, and other essential services, such as communications circuits and water.

1. Buildings or rooms housing uninterruptible power supplies will be accorded an appropriate level of physical and environmental protection. Any windows or large openings which can be used as a point of access shall be barred or screened to preclude surreptitious entry. Fuel tanks used to support emergency power sources should also be protected.

2. Other electrical facilities which support computer systems such as electrical closets and transformer vaults will be secured.

3. Terminal boards and other communications equipment associated with teleprocessing computer systems will be located in locked rooms to which access is strictly controlled.

3014. PROTECTION AGAINST THE EFFECTS OF MAGNETISM. While the hazards to magnetic computer storage media from magnets have received significant attention far beyond the real potential danger, possible disruption or damage to storage media from this source cannot be totally discounted. Where it is necessary to provide maximum protection against the potential effects of magnetic fields or radiation, all magnetic media storage containers should be kept at least 20 inches away from an exterior wall. This can be accomplished in the tape/disk library by maintaining a walking corridor around the room perimeter. Consideration should also be given to the adverse effect upon magnetic media placed in proximity to circuits that could serve as a conductor of lightning discharge currents.