Chapter 39 - Computer Systems and Facilities

3901 Protection of Automated Information Systems

A. Automated information systems and facilities require physical security measures to ensure proper and timely operation, to protect their value, to safeguard the integrity of information, and to ensure the safety of personnel. Computer systems and facilities and tape storage areas shall be protected from theft, alteration, damage by fire, dust, water, power loss and other contaminants, and unauthorized disruption of operation. The extent of physical security measures needed is determined by the results of a risk analysis and/or a physical security survey. Additional guidance for protection of automated information systems is provided in Chapter 10, Information Technology Security Programs of the Department's Information Technology Management Handbook.

B. The guidance and standards presented in this chapter are intended to protect physical assets and information, whether the information is classified, sensitive, or non-sensitive. The standards are directed generally at the dedicated computer facility. A computer facility is a single room or interconnected series of rooms that houses computer operations exclusively. Such operations consist of one or more computers with peripheral and storage units, central processing units, and communications equipment.

C. Security for microcomputers and other office automation equipment is covered later in this chapter. A security checklist for microcomputer users is in Appendix N, Physical Security Checklist for Personal Computer Users.

3902 Facility Design

A. A new computer facility can take advantage of new security systems and technology more readily than an existing facility because the installation of the security system would be more practical and cost-effective. The manager responsible for planning a new facility or the major renovation of an existing facility should review the considerations listed below. In addition to planning for security in the design phase, fire protection, and life safety provisions should be integrated into the design as well.

B. The facility should be located in the interior of the building and above ground level, preferably on the third floor or higher, for security and environmental reasons. The facility should be located. It should be separated from hazardous areas to decrease the possibility of fire, water damage, or loss

of power. Hazardous areas include mechanical rooms, laboratories, electrical or transformer rooms, printing rooms, trash bins, cafeterias, and parking areas.

C. The computer facility should be located away from high visibility, high traffic areas, such as entrances, lobbies, cafeterias, credit unions, and other support facilities. The hours of operation and identities of facility occupants should not be posted for public viewing. Additionally, the location of a computer facility should not be listed on a building directory.

D. To avoid having a computer facility unattended, a snack area and rest rooms may be located within the facility. However, these areas must be separated from operational areas. Food, drinks, and smoking should be prohibited near the computer equipment.

E. Computer facilities should be designated at a minimum as a "Controlled Area." A major computer facility should be designated as a "Restricted Area" in which access into the facility is limited to personnel who are assigned there or who are authorized access by the facility manager. See paragraph 3302, Area Designations, for further information regarding controlled and restricted areas.

3903 Walls and Windows

A. Walls forming the perimeter of the facility should be slab-to-slab or true floor to true ceiling. They should be constructed of substantial materials such as masonry or heavy plywood to prevent the spread of fire and surreptitious entry. The interior walls can be constructed of drywall or plaster board partitions.

B. From a security standpoint, windows are undesirable. If unavoidable, windows should be covered to prevent viewing of the facility's equipment, layout, and security protection hardware or systems. Also, they should be inoperable or secured to prevent opening. Windows at or below ground level should be protected with metal bars, metal screening, or alarm devices. Fastening devices should be located on the inside. Security alarms, panels, and sensors should not be visible from the windows.

C. An opening in the perimeter walls, other than a door or window, which is larger than 96 sq. inches or .06 sq. meters should be screened or grilled to prevent physical access to the facility.

3904 Doors and Locking Hardware

A. The number of doors should be limited to the minimum number required by:

1. The Code for Safety to Life from Fire in Buildings and Structures, National Fire Protection Association Publication 101, 2000 Edition.

2. Codes established by GSA's Public Buildings Service; and/or

3. Local building codes, as necessary.

B. A fire protection engineer can survey facilities, preferably in the design stage, to determine whether any doors can be permanently secured. All locked exit doors should be identified with signs prescribed by the applicable codes.

C. Perimeter doors should be constructed of solid wood or metal and without windows. Hinges should be mounted on the inside. If not, the hinges should be welded or peened to preclude removal. An astragal (a projecting strip on the edge of a door) should be mounted to protect the space at the lockset between the door and the strike. For doors with emergency exiting hardware, the astragal should be the full height of the door to preclude access to the panic bar by using a wire or other tool.

D. Perimeter doors should be locked when the facility is not attended or operational. High-security locking hardware should be used to secure the doors. A mortise lock or interlocking deadbolt rim-lock is recommended. Dead bolt latches should extend at least one inch or 2.54 cm into the strike plate or doorframe. Master keying should be minimized to promote effective key control. An automated information processing facility is a prime example of the need to minimize the number, control the distribution, and continually account for master keys as noted in paragraph 3504, Keys.

E. During hours of operation, a mechanical or electronic push-button combination lock or a card-activated access system should be used to save wear on the high security locking hardware. When using the combination lock, ensure that someone standing nearby cannot observe the combination being entered. Refer to Chapter 35, Locks and Keys, for more information on locks and locking systems.

F. Other options include a wide variety of card reader locks. High-security areas may require supplemental measures such as a guard post and a visual identification access control system.

3905 Access Control

A. Access to a computer facility must be controlled, but acceptance of security measures and cooperation by occupants are essential for effective access control. Access should be limited to personnel responsible for operation, maintenance, or management of the computer and its support systems. Users do not normally need access to the computer room.

B. Physical access control systems incorporate elements such as proximity sensing card readers, biometric systems, electronic card key readers, push-button combination locks, key locks, and identification badge systems. Since each system comes in a variety of designs, the computer facility manager, in close consultation with the servicing security officer, should explore systems from a variety of vendors to find the type to meet the needs of the facility.

C. Visitors to a facility should provide photo identification and complete the visitor register. Visitors should be escorted at all times in a facility that processes sensitive or classified information.

D. Refer to paragraph 3908, Personal Computers and Office Automation Equipment, regarding access to microcomputers and other office automation equipment.

3906 Fire Protection

A. In virtually every computer facility, some kind of fire protection system is necessary. In addition to having fire extinguishers at hand and in well-marked locations, installation of a fire detection and suppression system must be considered. System specifications should be based on the size of the facility, the type and amount of hardware in place, the criticality and sensitivity of the operations, applicable codes, and cost. Such a system must be properly maintained and tested periodically. Detection systems of choice are ionization-smoke and fixed-temperature heat.

1. The primary suppression systems are water sprinklers. Water sprinkler systems are of the dry or wet type. The dry system maintains water pressure at a valve, not in the pipes or at the sprinkler heads. The dry system mitigates any concern for leakage or spontaneous release.

2. Halon systems are supplemental to water systems. Halon systems in place may remain subject to conditions. Maintenance of the system may continue as long as the service does not require replacement of Halon. Halon may no longer be manufactured and any remaining stock will not be used. Should the system be activated, or as a part of routine maintenance need suppressant, the replacement must be a Clean Agent. Use of any Clean Agent, which replaces Halon, requires costly modification to the system. Replacing this system would be more economical. Water sprinklers can be used as the single fire protection system, GSA does not require a supplemental suppression system.

3. Portable fire extinguishers should be installed in the computer facility to put out small or smoldering fires of any type. The common types of extinguishers are CO^2, dry chemical, or water. Select dry chemical to ensure coverage for types A, B, and C fires. The extinguishers should be located at points that are easily accessible in an emergency. A visible marker should

be placed high enough above the extinguisher to be seen over the computer equipment. Guidance for extinguisher management may be found in NFPA 10, Standards for Portable Fire Extinguishers, and Chapter 2, Fire Protection, GSA/PBS, 5099.2, Safety and Environmental Management Program.

B. The facility's fire protection system, including detectors, water pumps and exit signs, should have a dedicated power source. The system should also have emergency and/or battery backup power sources. Conversely, the external facility alarm system should annunciate within the computer facility for the safety of personnel working inside. When activated, it should automatically cut the power to the computer equipment and air handling system, but not the lights. Sensors should be installed in the ceiling, below the raised floor, and in return air ducts. These sensors should detect both heat and smoke. Testing of the system should be conducted at least annually.

C. Fire alarm systems notify occupants and a response force of an emergency condition. To be most effective, a local alarm must be centrally located in the facility and be loud enough to be heard above the normal noise levels in all areas of the facility. Most fire codes require an 85 decibel (db) sound level within ten feet/3.05 meters of each aural device. Any fire alarm system must make provisions to notify aurally and/or visually impaired persons. The alarm should also be designed to initiate a response from the local fire department. To accomplish this, a guard force, a contract monitoring station, an automatic dialer, or the fire department, can monitor the alarm. The computer facility manager must make provisions for unimpeded access to all parts of the facility to minimize any damage resulting from delays in getting fire fighters or equipment to the scene.

3907 Data Storage Areas

Storage media must be protected to preserve the value and integrity of the information or to prevent its disclosure. Having the data storage area and the computer system in the same facility is convenient but it increases the vulnerability to loss if the fire suppression system is activated. Storage areas are safer when located away from the computer facility. Access of personnel into data storage areas should be controlled the same as that for a computer facility. Also, the same fire protection, environmental controls, and housekeeping practices should be provided.

3908 Personal Computers and Office Automation Equipment

A. Personal computers and office automation equipment have proliferated throughout the Department. They are becoming more portable and compact. Information that was once on paper is now in electronic form and placed on disks. The disks are either removable or built-in. Where once we were only concerned with locking up paper, we now must protect computer hardware, software,

and information. The person who uses the computer is responsible for the following protective measures.

- Managing passwords in accordance with the "DOC Policy on Password Management" to control user authentication to IT systems.

- Preventing unauthorized access to equipment. When leaving the room where the equipment is located, individuals should lock the door. Where practical, a locking device that anchors the unit directly to the desk may be used. Other devices include keyboard locks that disable the electronics, and cabinet locks to secure the equipment out of sight.

- Ensuring that all hardware is marked with identifying information and reporting unmarked equipment to the unit's property custodian. This will assist in deterring thefts and will facilitate tracing missing items for recovery.

- Locking removable diskettes and hard drives in secure containers. Users should make back-up copies of important files stored on their PC workstation.

- Keeping an inventory of computer equipment and removable diskettes. Supervisors and managers should establish a system of accountability and direct the unit property custodian to periodically conduct inventories of the equipment.

- Not storing excess, unassigned, or unused equipment in the open or in isolated areas. Such equipment should be stored in secured rooms or cabinets, readily available but out of view of unauthorized persons. Assigned equipment must be protected by locking office doors when visual protection is not available or practicable.

- Utilizing property passes for the control of all property being removed from the facility or building. See Chapter 33, Interior Protection, for details on property control.

- Not releasing hardware components for repairs without a written repair order that includes a description of the equipment and the identity of the person who requested the repair.

- Checking the identification of all repair personnel and other vendors. Do not let them roam in the computer area alone, even if they are known. A transmitter chip easily installed by a hostile repairman can transmit every computer transaction to a remote receiver.

- Reporting thefts immediately to the servicing security officer or guards and to the Information Technology Security Officer. Be able to report the make, model, serial number, and description of the equipment.

B. A Physical Security Checklist for PC Users is attached at Appendix N.