Chapter 33 - Interior Protection

3301 Interior Security Controls

A. The second line of defense of the perimeter is interior controls. When an intruder is able to penetrate the perimeter controls and the building exterior, the interior controls must be able to stop further penetration. There are few facilities where every employee has access to every area in the facility. Accordingly, access to some areas will be controlled. For example, interior controls are necessary to protect classified information from unauthorized disclosure, to prevent damage to the area or to equipment, to prevent interference with operations, for safety purposes, or for a combination of these reasons.

B. Interior controls are applied to specific rooms or physical spaces within a building or facility. The facility or office manager is responsible for determining whether interior controls are necessary. Office area controls include structural upgrades, key accountability systems, locking devices, and access control systems.

C. The extent of interior controls will be determined by considering the monetary value and mission criticality of the items or areas to be protected, the vulnerability of the facility, and cost of the security controls. Normally, the cost of security controls should not exceed the value of the item or area to be protected.

3302 Area Designations

A. Controlled Area. A controlled area is defined as a room, office, building, or other form of facility to which access is monitored, controlled, or restricted. Admittance to a controlled area is limited to persons who have official business within the area. The senior facility manager, in consultation with the servicing security officer, is authorized to designate an area as a controlled area after adequate security measures are in place. The following areas shall be designated as controlled areas.

1. An area where classified information or highly sensitive information is handled, processed, or stored. For example, a mailroom is considered a controlled area.

2. An area that houses equipment that is valuable or critical to the continued operations or provision of services.

3. An area where uncontrolled access would interfere with or disrupt personnel assigned to the area in carrying out their official duties.

4. An area where equipment or operations constitute a potential safety hazard.

5. An area that is particularly sensitive as determined by the facility manager.

6. Law enforcement offices.

B. Restricted Area. A restricted area requires special constraints or controls to safeguard property or material. Admittance to a restricted area is limited to personnel assigned to the area and persons who have been specifically authorized access to the area. Personnel without an appropriate security clearance must be escorted in a restricted area where classified material is produced, processed, or stored by personnel assigned to the area. When uncleared personnel are present in a restricted area, classified information must be protected from observation, disclosure, or removal. The facility manager, in consultation with the servicing security officer, is authorized to designate an area as a restricted area after adequate security measures are in place. The following areas shall be designated as restricted areas.

1. Any area housing Top Secret information (see paragraph 3306, Security Vaults, and paragraph 3307, Security Vault Doors, regarding vaults and strongrooms).

2. Any area accredited for the open storage of Secret or Confidential classified information. This includes areas where classified information is normally or frequently displayed, such as charts, maps, drawings, photographs, equipment, or conference rooms where classified information is being discussed. This does not include an office in which classified information is discussed or displayed and action can be taken by occupants to prevent disclosure.

3. An area used as a major repository for classified materials or where classified materials of substantial volume are produced or handled.

4. A telecommunications center that processes classified information.

5. An area that conducts client-server computer operations or highly valuable or sensitive equipment.

6. Law enforcement evidence rooms and weapons/ammunition storage areas as appropriate.

7. Any other area that is highly critical or sensitive as determined by the facility manager.

C. Working and Storage Areas for Special Access Programs.

1. **SCI Facilities.** A protected room or office where Sensitive Compartmented Information (SCI) may be stored, used, discussed, and/or processed is called a Sensitive Compartmented Information Facility or SCIF. There are two types of SCIFs: working areas and storage areas. Prior to formal accreditation, the area must meet the rigid physical security standards set forth in Director of Central Intelligence Directive (DCID) 1/21, Physical Security Standards for Sensitive Compartmented Information Facilities. The Office of Security provides liaison with other government agencies on security matters and coordinates the accreditation of SCIFs within the Department.

2. **Other Special Access Program Areas.** Government agencies outside the Intelligence Community may have special access programs that require stringent physical security standards. Working and storage areas in the Department where special access program information is stored, used, discussed, or processed will be constructed in accordance with standards issued by the sponsoring agency. The Office of Security will coordinate the approval process with the appropriate agency. To initiate the process, an operating unit head shall submit a written request with justification to the Office of Security.

3. **Accreditation of Facilities.** SCI material can be maintained only in facilities approved by the CIA for its receipt, storage, and handling. To request establishment and accreditation of a SCIF, a request should be forwarded through the Department's Office of Executive Support (OES) to the Office of Security. The request must include the SCI level of accreditation requested, complete address, point of contact, justification, and a description of any automated equipment that will be housed in the area. Based on the request, the Office of Security will conduct a physical security survey of the facility to be accredited as a SCIF. Recommendations for any security upgrades will be provided to the requester. After implementing the recommendations, a follow-up inspection will be conducted prior to final accreditation. A final accreditation shall be provided in writing to the operating unit head, the operating unit's security contact, and the servicing security officer with a file copy maintained in the Office of Security.

3303 Challenge Authority

Any person within a departmental facility, regardless of position, shall be subject to challenge by another departmental employee, the servicing guard force, security contact, servicing security officer, or any law enforcement officer, and shall display appropriate identification when challenged. Failure to do so may result in removal from the facility or other administrative action.

3304 Property Control

Facility and office managers shall establish procedures for the control and accountability of property in departmental facilities in accordance with existing Federal property regulations. The following documentation is used for property control.

A. Optional Form 7, Property Pass.

1. GSA regulations require that all property leaving Federal facilities be accompanied by proof of authorized possession or ownership. The form presently in use nationwide for this purpose is the Optional Form 7, Property Pass. This form is available through Commerce supply stores and at GSA Self-Service Supply Centers.

2. The first step in establishing a Federal property control program is to establish a cadre of officials who are authorized to sign the Optional Form 7. This list must be updated periodically and should be provided to the guard force or to other individuals who control facility entrances. The authorized signers should be supervisors or administrative officers who are in a position to have some familiarity with the items most likely to be removed from their respective areas. They should be instructed in how to fill out the forms, how to clearly identify property, and how to maintain an accountability and follow-up program to assure the return of Federal property.

3. The guard force post orders at each entrance should set forth the procedures for checking outbound property, for identifying property by serial number and description, for verifying authorized signatures, and for retrieving the Optional Form 7 when the property passes their post. They should also have instructions on how to deal with individuals who do not have the proper documentation when attempting to remove property. The guards should return all retrieved Optional Form 7s to the appropriate security official at least every 30 days.

4. The security contact should forward the retrieved Optional Form 7s to the authorized signers for follow-up action to ensure that removed Federal property is properly accounted for and returned.

5. Security contacts or facility managers may wish to expedite the property control process in larger facilities by establishing a sign-in/sign-out log. Such a procedure will permit visitors to bring property into the building and leave the building the same day at the same entrance without having to obtain a property pass.

B. Other Forms for Removing Property. In addition to the Optional Form 7, the following documentation may be used for removing the referenced materials from Commerce facilities.

1. **CD-50, Personal Property Control.** This form is used to request and account for the moving or disposal of furniture, office equipment, and other personal property from and between Commerce facilities.

2. **CD-10, Publications Service Request.** This form may be used to document and authorize the removal of official printed matter such as supplies of forms, pamphlets, and other Department of Commerce published documents.

3. **Sales Receipt.** A sales receipt or other documentation that provides proof of ownership for personally owned property.

3305 Intrusion Detection Systems

A. Purpose. Alarm systems are designed to alert security personnel or other staff of an actual or attempted intrusion into an area. These warning systems detect and report intrusions or attempts to breach a specific area. All alarm systems require a response capability to provide real protection for an area. All systems have weak points by which their effectiveness can be minimized or even completely interrupted or circumvented. Proper design and routing of cables can minimize this risk. The advantages and limitations of a variety of detection systems are described below.

B. Planning Alarm Installations. Alarms are used to detect approach or intrusion into an area. Some alarms are intended for exterior protection and others are suitable only for indoor installations. The following criteria must be addressed in determining the need for an alarm system.

1. Sensitivity or criticality of the operation.

2. Vulnerability of the facility to damage, interruption, alteration, or other harm.

3. Sensitivity or value of the information or property stored at the facility.

4. Location of facility and accessibility to intruders.

5. Other forms of protection in place or available.

6. Response capability of the guard force or local law enforcement units.

7. Number of staff needing access to protected areas.

C. Components of an Alarm System.

1. **Alarm Panel.** An analog computer inside a steel cabinet that receives signals from individual sensors and zones. The computer normally uses a telephone line to report administrative and alarm activity to a monitoring station.

2. **Alarm Sensors.** Devices that use magnetic, infrared beam, acoustical, shock, microwave, photoelectric, or moisture sensors to detect physical presence in an area. Each sensor uses a different type of technology.

3. **Alarm Annunciators.** A device that provides a sound and/or a visual signal to activate a system's alarm or indicate a system's malfunction. Annunciators may be combined in a system that announces alarms both locally and remotely.

4. **Emergency Electrical Backup.** A DC power system that provides a supply of power to ensure continued protection in case of electrical (AC) power loss. Normally enough battery capacity is provided for up to 48 hours of operation with one hour of annunciation activity.

5. **Alarm Addressing.** A device used to identify and define zones in the security system. Typically, one or more devices may be addressed to a specific zone. All devices on a zone should use the same type of technology.

D. Alarm Annunciation. For an intrusion detection system to be effective, the alarm must annunciate, or sound, at a time and location that will generate a satisfactory response. Alarm devices use transmission lines or radio communications to relay a warning of intrusion or potential danger. Types of annunciation include the following devices.

1. **Local Alarm System.** The local alarm system has circuits within the secured area that are directly connected to audio or visual signal-producing devices such as annunciator panels, bells or sirens, or a staffed monitoring station located in the protected facility. Devices that do not annunciate at a panel should be mounted on the exterior of the building or, in large buildings, at interior locations where they will be audible or visible at a reasonable distance. Any alarm system should be protected against weather and tampering.

2. **Central Alarm System.** The central station receiver is connected to an alarm through telephone lines, long-range radio, cellular phone systems, or direct wire. Central alarm systems can generate a response to a centrally located station such as a local police station or a commercial central alarm station service that provides monitoring services. When an alarm is activated, the monitoring station initiates a response either by calling personnel designated for

the area or by dispatching guards to the location. The response time for alarms of this type should not exceed ten minutes.

E. Types of Alarm Devices.

1. **Magnetic Contacts.**

a. Magnetic contacts consist of a magnet and a reed switch. When the magnet and the reed switch are aligned the contact is secure. When they are not aligned the contact is considered open. End-of-line resistors will be used to indicate if a wire is cut when the proper signal is not received. Magnetic switches can either be flush or surface mounted. Surface mounted contacts are mounted on the inside of a door or opening to be protected. Flush mounted contacts are positioned with the magnet in the area that pivots (e.g. door) and the reed switch in the stationary frame surrounding the opening.

b. Balanced magnetic contacts will be used in high-security applications. These contacts and magnets are manufactured with matched magnet and reed switch. This ensures another magnetic field cannot be used to indicate the protected opening is secured.

2. **Passive Infrared Devices.**

a. Passive infrared (PIR) detection devices are best used in an interior environment. Wall mounted passive infrared detection devices work best in an expansive area since the infrared beams spread with distance. Ceiling mounted passive infrared detection devices should be used to provide protection in office spaces. Ceiling mounted devices allow for movement of furniture without diminishing the coverage. Configuration of devices should be so that one provides coverage for one assigned zone. This provides a definitive location for the alarm. All passive infrared passive devices should be supervised through the use of end-of-line resistors.

b. PIR detection devices typically have a wire hole or knockout to allow the device to be wired. This hole shall be sealed with a flexible sealant such as caulk after it is wired. This will prevent insects and moisture from getting into the device.

c. PIR detection devices shall be walk-tested to assure adequate coverage. Normally a red light will flash in the detection device when it picks up a heat source. The heat source (e.g. human, large dog, etc.) will trigger the light within the designed range of the PIR detection device.

d. The use of ceiling mounted passive infrared detection devices is highly recommended. Such use helps to eliminate blind spots in coverage when offices are internally reconfigured. This is especially useful when office furniture is periodically moved.

e. **Advantages:** Infrared detection devices can be used to activate other security devices, such as cameras or microphones. Passive infrared detection devices can also radiate beams 360 degrees.

f. **Disadvantages:** Infrared detection devices do not pick up body heat when the ambient temperature is below 38 degrees Fahrenheit.

3. **Dual Technology Passive Infrared and Microwave Sensors**.

a. Dual Technology Passive Infrared and Microwave Sensors use two distinct technologies to provide reliable detection. Essentially, a dual technology passive infrared and microwave sensor will not generate an alarm unless both the passive infrared and microwave technologies agree there is an intrusion. Additionally, the sensors have built in line-supervision of both technologies in case of unit failure.

b. **Advantages:** Dual technology passive infrared and microwave sensors are compact and easily installed, provide good coverage, are difficult to detect, have high salvage value, and are not affected by air currents, temperature, noise, light, or sound.

c. **Disadvantages:** The initial cost for dual technology passive infrared and microwave sensors is high.

4. **Audio Alarm Devices.**

a. Audio alarm devices use a microphone and a microprocessor to detect the breakage of glass. This detection is a two-phase event. The "thud" of the window being hit (400 - 600 kHz) opens the microphone to see if the glass is actually broken (19,000 kHz). These sensors are supervised and are extremely reliable. Water is the only external influence that would degrade this type of sensor.

b. **Advantages:** Audio alarm devices have minimal installation costs, high reliability, and a 10-year life span.

c. **Disadvantages:** Line-of-sight must be maintained between the audio alarm device and the glass protected. The use of heavy curtains may result in more sensors being installed, which would add more cost to properly alarm an area.

5. **Seismic Detection Devices.**

a. Seismic devices are sensitive to vibrations within the wall or structure upon which they are mounted. They have many of the same capabilities as microphones.

b. **Advantages:** Seismic detection devices are easy to install and offer effective protection for vaults.

c. **Disadvantages:** Although vibrations caused by passing vehicles or falling objects may trigger seismic detection devices, the devices can be adjusted over a period of time to compensate for false readings.

6. **Closed Circuit Television.**

a. Closed circuit television (CCTV) is not primarily an alarm device but rather a monitoring device. It is frequently used as an access control measure or as a supplement to other alarms or access control systems. CCTV systems can be used at multiple locations where visual monitoring from a remote location is advantageous, such as gates, doors, corridors, elevators, and other areas where it is not practical or cost effective to post a guard. When a CCTV system is in place, the system signals shall be recorded by a videotape system for playback and analysis at a later time. The system shall be used in conjunction with a time/date generator that projects a continuous image of the date and time in a corner of the monitor screen. System features should include a time-lapse mode for quick playback of lengthy periods of taped coverage. Switching or multiplexing equipment must be provided in conjunction with the VCR to permit multiple screen recording and playback. When funds permit, color monitors should be considered to enhance the quality of personnel identification.

b. **Advantages:** One individual at a central station can monitor several CCTV camera locations simultaneously, and the visual image conveys much more information than other types of alarm systems.

c. **Disadvantages:** CCTV monitors do not normally provide an alarm to alert the observer, and the attention of persons monitoring television images at central stations can be distracted.

7. **Closed Circuit Television as a Detection Device.**

a. CCTV systems can be used as a detection device to trigger alarms under certain circumstances, much like space alarms where motion detection is desirable.

b. A signal generator attached to the monitor can be adjusted to project a pattern of light or dark rectangles, or windows, which can be adjusted in size and location on the screen. The windows can be focused on a fixed object to be protected or alarmed such as a safe or a doorknob. When the image of an intruder or moving object enters the window, the difference in contrast is detected and triggers an alarm.

8. **Capacitance Alarms.**

a. A capacitance alarm is used to protect specific objects such as security containers and safes. The capacitance alarm uses the metal construction of the container and causes it to act as a capacitor or condenser. When a change occurs in the electromagnetic field surrounding the metal object, the balance is disturbed and an alarm is activated. The protective field on the container is usually kept to a distance of not more than a few inches/centimeters from the surface of the safe. This prevents unwanted alarms activated by authorized individuals passing within a few feet/meters of the container. Very close proximity or contact with the protected object will set off the alarm.

b. **Advantages:** Capacitance alarms are compact in size, simple to install, easy to operate, and provide a high degree of security. Operating in an invisible protective field, capacitance alarms make it difficult to determine what is being protected. Several containers in the same area can be connected to one system.

c. **Disadvantages:** Capacitance alarms can only be applied to ungrounded equipment. Accidental alarms can occur if someone touches the container.

F. Line Supervision. The telephone or dedicated lines that transmit the alarm signals from the protected area to the monitoring station must be protected to prevent interruption of the alarm signal. To ensure such integrity, the transmission lines should be electronically supervised.

1. Annunciator panels usually come equipped with relays to detect changes in signal strength, although they may not be sensitive enough to detect minuscule changes. Signal line tampering can usually be detected if a low tolerance to electrical resistance is maintained in the lines. Systems having supervision tolerances under 25 microamperes are quite effective.

2. Line supervision can be a weak link in the alarm system and should be given as much attention as other components. Accurate and complete records should be kept of all nuisance alarms.

3306 Security Vaults

A. Purpose. A vault is a completely enclosed space with a high degree of protection against forced entry. Security vaults are commonly used for storing Top Secret information, Special Access Program information, classified communications equipment, and materials with a high dollar value.

B. Construction Criteria.

1. **Reinforced Concrete Construction.** A vault is constructed to rigid specifications. Walls, floors, and ceiling will be a minimum thickness of eight inches of reinforced concrete. The concrete mixture will have a comprehensive strength rating of at least 2,500 pounds per square inch. Reinforcing will be accomplished with steel reinforcing rods, a minimum of 5/8" in diameter, positioned in the concrete mixture and spaced horizontally and vertically six inches on center; rods will be tied or welded at the intersections. Each reinforcing rod is to be anchored into the ceiling and floor to a minimum depth of one-half the thickness of the adjoining member.

2. **GSA-Approved Modular Vaults.** Modular vaults meeting Federal specifications may be used in lieu of the above criteria. Modular vaults are flexible, movable, and expandable, and can be configured to unique space requirements. Class M vault systems accommodate Class 5 GSA-approved vault doors and are recommended by GSA for classified information and material, data, and security communication devices. The systems are accredited by National Authority for use as a SCI facility.

3. **Steel-Lined Construction.** Where unique structural circumstances do not permit construction of a concrete vault, construction will be of steel alloy-type of 1/4" thick, having characteristics of high yield and tensile strength. The metal plates are to be continuously welded to load-bearing steel members of a thickness equal to that of the plates. If the load-bearing steel members are being placed in a continuous floor and ceiling of reinforced concrete, they must be firmly affixed to a depth of one-half the thickness of the floor and ceiling. If the floor and/or ceiling construction is less than six inches of reinforced concrete, a steel liner is to be constructed the same as the walls to form the floor and ceiling of the vault. Seams where the steel plates meet horizontally and vertically are to be continuously welded together.

C. Security Vault Doors.

1. Security vault doors are classed by their security ratings as established by GSA. All vaults shall be equipped with a GSA-approved Class 5 or Class 8 vault door (see Federal Specification AA-D-00600C). Within the United States, a Class 6 vault door is acceptable. Normally within the United States, a vault will only have one door that serves as both entrance and exit to reduce costs.

2. Security vault door criteria in the Department will be that as listed in the DCID 1/21, Physical Security Standards for Sensitive Compartmented Information Facilities. For further information concerning specifications and installation requirements refer to DCID 1/21, Chapter 31.

3. Every vault door should be equipped with an emergency escape device. The escape device, not activated by the exterior locking device, should be accessible on the inside only and should be permanently attached to the inside of the door to permit escape by persons inside the vault. The device should be designed and installed so that drilling and rapping on the door from the outside will not give access to the vault by actuating the escape device. Vault doors conforming to Federal specifications will meet this requirement.

4. A decal containing emergency operating instructions should be permanently affixed on the inside of the door. Each vault should be equipped with an interior alarm or device (such as a telephone, radio, or intercom) to permit a person in a vault to contact the vault custodian or guard for assistance. Further, the vault should be equipped with a luminous-type light switch and, if the vault is otherwise unlighted, an emergency light.

3307 Strongrooms

A. Purpose. A strongroom is an enclosed space constructed of solid building materials used to store sensitive material or high-value items in a shipping and receiving facility. Protection is normally supplemented by guards or alarm systems. Rooms that have false ceilings and walls constructed of fibrous materials or other modular or lightweight materials cannot qualify as a strongroom.

B. Construction Standards.

1. Heavy-duty builder's hardware shall be used in construction. All screws, nuts, bolts, hasps, clamps, bars, hinges, and pins should be securely fastened to preclude surreptitious entry and to assure visual evidence of forced entry. Hardware accessible from outside the strongroom must be peened, brazed, or spot-welded to preclude removal.

2. Walls and ceilings should be made of plaster, gypsum board, metal, hardboard, wood, plywood, No. 9 gauge or heavier two-inch/5.08 cm wire mesh, or other materials of sufficient strength or thickness to deter entry and/or give evidence of unauthorized entry. Insert-type panels should not be used.

3. Floors should be solidly constructed using concrete, ceramic tile, or wood.

4. Windows should be fitted with 1/2" or 1.27 cm horizontal bars (six inches or 15.24 cm apart) and cross bars to prevent spreading. In place of bars, No. 9 gauge wire mesh can be fastened by bolts extending through the wall and secured on the inside of the window board. Windows should be kept closed and made opaque by any practical method, such as paint on both sides of the window, tempered masonite, sheet metal, or wallboard.

5. Where ducts, registers, sewers, and tunnels are of such size and shape as to permit unauthorized entry, they should be equipped with man-safe barriers such as wire mesh (No. 9 gauge, two-inch or 5.08 cm square mesh) or steel bars of at least one-half inch or 1.27 cm diameter extending across their width with a maximum space of six inches or 15.24 cm between the bars. The steel bars should be securely fastened at both ends to preclude removal, with cross bars to prevent spreading. Trap doors should be dead-bolted inside the room.

6. Doors should be constructed of metal or solid wood. When doors are used in pairs, an astragal (overlapping molding) should be used where the doors meet. When the construction is of No. 9 gauge, two-inch or 5.08 cm wire mesh, a similarly constructed door can be used; however, the wire mesh door should be reinforced with a metal panel at least 36 inches or .91 meters wide, from floor to ceiling, welded to the inside of the wire-mesh wall to protect the locking device from unauthorized access or tampering.

7. Door louvers and baffle plates shall be reinforced with No. 9 gauge, two-inch or 4.08 cm square wire mesh fastened to the inside of the door.

8. The doors to strongrooms should have a computerized combination lock meeting Federal Specification FF-L-2740.

9. Depending on the value and/or sensitivity of the items contained in the strongroom, consideration should be given to the installation of a more comprehensive intrusion detection system.