

Section 5

BARRIERS

Contents

References	5-1
General Information	5-1
Common Deficiencies/Potential Concerns.....	5-2
Planning Activities.....	5-3
Performance Tests.....	5-4
Data-Collection Activities.....	5-4

References

DOE Order 5632.1C
 DOE Order 6430.1A
 DOE Manual 5632.1C-1

General Information

Physical barriers are used to control, impede, or deny access, and effectively direct the flow of personnel and vehicles through designated portals. Barrier system effectiveness is based on whether it complies with DOE orders and whether performance testing indicates that the system performs adequately.

Specifically, barriers are designed to reduce the number of entry and exit paths, facilitate effective use of protective force personnel, delay the adversary to enable assessment, protect personnel from hostile actions, and channel adversaries into preplanned neutralization zones.

The following subject areas are addressed in this section:

- Fences
- Buildings (walls, ceilings, floors, doors, windows, and unattended openings)
- Locks and security containers
- Denial systems
- Vehicle barriers.

Fencing is normally used to enclose security areas and to designate DOE property boundaries. Depending on the level of security required,

fences require regular patrolling, continuous observation, or an intrusion-detection system supported by an assessment capability. DOE requires that fences meet specific gauge and fabric specifications, be topped with particular wire and outrigger configurations, include steel posts with bracing, and meet certain height and location provisions.

Buildings of various types represent the most common barrier used to protect DOE security interests. Construction features vary throughout the DOE complex; however, there are a number of basic requirements to consider when evaluating walls, ceilings, and floors used to enclose security areas. In general, it is important that building materials be solid and offer penetration resistance to, and evidence of, unauthorized entry. Shatter-resistant, laminated glass of a minimum thickness may be used if visual access is required. DOE orders and manuals provide requirements for a variety of construction elements, including wire mesh, insert panels, sound attenuation, storage rooms, and wall configuration for rooms in which classified information is to be discussed. There are also specifications for construction hardware; for example, hardware accessible from the outside is required to be peened, brazed, or spot-welded to preclude tampering or removal.

In addition to the criteria for walls, ceilings, and floors, there are requisite construction requirements for doors, windows, and unattended openings. It is important that doors offer resistance to forced entry and, when necessary,

reinforcement is required for doorjamb, louvers, and baffle plates. Windows, when relied on as physical barriers, must be constructed of shatter-resistant, laminated glass of a minimum thickness, and installed in fixed frames so that the panes are not removable from the outside. It is essential that window frames are securely anchored in the walls, and that windows can be locked from the inside. Unattended openings, under certain conditions, are to be alarmed or equipped with steel wire mesh and steel bars with steel crossbars, which are checked for integrity during patrols.

The requirements for security locks are determined in light of the security interest being protected, the identified threat, existing barriers, and other protection measures. Security containers used for Top Secret National Security Information (NSI)/Restricted Data (RD)/Formerly Restricted Data (FRD) and Category I SNM must use locks that meet Federal Specification FF-L-2740. All other security containers used to protect information below Top Secret NSI/RD/FRD and below Category I SNM must use locks that meet Military Specification MIL-L-15596G or Federal Specification FF-L-2740, depending on lock performance and whether it was produced before or after October 1, 1991.

Combination locks must meet Federal Specification FF-P-110 and Standards cited in 41 CFR Chapter 101. Key padlocks are required to meet certain military specifications, depending on whether they are high-security, medium-security, or low-security padlocks. Also, there are requirements for key locksets, lock bars, hasps and yokes, electromagnetic locks, and panic locks.

The General Services Administration (GSA) establishes standards for security containers. Although classification is the only security factor that determines the degree of protection required for classified matter in storage, other considerations pertain, such as strategic importance, susceptibility to compromise, effect on vital production, health and safety factors, and replacement costs. Other DOE requirements address protective force inspections and patrols, transfer of security containers, protection of

security containers and combinations, and security repository information.

Active denial systems include obscurants (smoke) and other dispensable materials, such as foam, sprays, and irritant agents. It is important that they be protected from tampering and be properly maintained. Other systems may incorporate flickering light or intense sound systems to delay, confuse, or otherwise hamper adversaries.

Vehicle barriers are used to deter penetration into security areas when such access cannot otherwise be controlled. Vehicle barriers may include pop-up barriers, cable, bollard configurations, or natural terrain obstacles (for example, bodies of water, ravines, steep hills, or cliffs).

Common Deficiencies/ Potential Concerns

Fences

To be effective, fencing must be checked and repaired on a regular basis. Frequently, the fence fabric is not properly attached to the support poles and the bottom wire is not secure. Erosion of the ground under the fence often results in gaps or washouts that may permit someone to crawl under the fence. Another common problem is that vegetation is allowed to grow up close to the fence providing cover to potential adversaries or a possible platform for climbing over the fence.

Buildings

Suspended ceilings and raised floors often create the illusion that they represent the “hard” surfaces of the enclosed space. Inspectors often overlook these configurations. The ceiling and floor panels must be inspected to ensure that the true “hard” walls and surfaces of the building are identified. This is especially important in locations where such walls form a PA or MAA boundary (e.g., entry control facilities).

Locks and Keys

Many of the locks used for security purposes are advertised as “high-security” or “medium-security” locks. When examined, it is often

revealed that the lock specifications do not meet the required MIL standards or DOE requirements. Inspectors should be aware that these terms, high security and medium security, when used commercially may not have the same implication as they do in DOE orders.

Effective control must be maintained to assure that locks and keys are used appropriately. Combinations must be changed at specified times and under specified conditions, and key control procedures must be documented and followed. Appropriate procedures for dealing with lost keys must be established.

Security Containers

Some facilities have requested and received exceptions for the use of non-GSA-approved containers for the storage of classified documents. Inspectors should not assume that all facilities have these exceptions. All exceptions received by the inspected facility should be reviewed before the onsite inspection to determine whether they are current.

Denial Systems

A form of denial system used at some DOE facilities consists of an extremely heavy block of concrete placed in front of an access door to protect classified weapons or components. To gain access, a hydraulic vehicle or some other lifting mechanism must be used to move these barriers. Since these vehicles or mechanisms become a critical factor in the application of this kind of barrier, they must be afforded an effective degree of protection. Inspectors should check to ensure that these items of equipment are being appropriately protected and properly maintained.

Vehicle Barriers

Vehicle barriers must be effectively monitored, and components must be appropriately located. Barriers should be within the area being protected by detection sensors.

Activated Denial Systems

Adequate protection must be provided to prevent an insider from disabling activated denial systems

(such as cold smoke or sticky foam). Since most such systems have a single location for firing, they represent a vulnerability to insiders unless sufficient protective measures are employed.

Planning Activities

During the planning meeting, inspectors should interview points of contact and review available documentation relative to the presence and use of barriers. This documentation should include building construction drawings, focusing on barrier construction details and heating, ventilation and air-conditioning ducts. Elements to cover include:

- The general types of barrier systems (e.g., fences, standard building materials, reinforced/hardened building materials) in place at each security area, including:
 - Property PA
 - LA
 - Exclusion area
 - SCIF
 - Secure communications center
 - Vital area
 - PA
 - MAA
- The types of barrier systems associated with the various storage/process areas (e.g., vaults, safes, vault-type rooms) used to protect SNM, vital equipment, and classified matter. In particular, determine:
 - Whether activated denial systems (e.g., smoke, foam) are used
 - Whether items within storage areas (e.g., vaults) are protected by additional controls (e.g., locked compartments, tie-downs)
 - Methods for providing delay when material is in use and when storage areas are in the access mode
 - Interfaces with entry controls and intrusion-detection systems

- Whether airborne denial systems are in place in any areas
- The types and locations of vehicle barrier systems
- The type(s) of lock systems used (e.g., key locks, padlocks, combination locks, door strikes, magnetic locks) and the organizations (e.g., protective force, material custodians, production organization, health physics) that control and maintain keys or combinations to lock systems, as well as the general responsibilities of each organization (e.g., protective force has keys to MAA doors, whereas custodians have combinations to vault doors).

Performance Tests

There are no performance tests directly relevant to this subtopic. The use of performance test results to identify delay times is discussed in item N under Data-Collection Activities.

Data-Collection Activities

General

A. Inspectors should determine whether barriers at facilities with Category I SNM or vital equipment provide sufficient delay to allow the protective forces to assess alarms and respond with sufficient force to neutralize the adversaries before they have completed their intended purpose. (This is generally evaluated based partially on a review of the vulnerability assessments.)

B. Inspectors should determine whether barriers at SNM areas, vaults, and MAA perimeters are sufficient to ensure that SNM cannot be removed from the area without causing an alarm or immediate visual evidence of tampering. Also, inspectors should determine whether barriers are sufficient to channel personnel through designated portals or into adversary neutralization zones.

Perimeter Barriers

C. For security areas where a perimeter barrier system is used, inspectors should determine what types of barriers are in use (fences, wire, vehicle barriers, or natural obstacles), whether they meet DOE requirements, and whether all barriers have been accurately represented in vulnerability assessments and in the SSSP. Inspectors should determine whether there are procedures in place to prevent transferring contraband or special nuclear material over an exterior perimeter barrier (for example, throwing or slinging items over a fence for later pickup). Preventive measures may include wide isolation zones, extra high fences or nets, or adequate surveillance by protective force personnel.

D. Inspectors should examine fences to determine whether their condition would allow adversaries to get through or bypass them without being detected. Some items to consider include:

- Erosion in isolation zones or under fences that may create a condition that would allow an adversary to pass undetected
- Unprotected pipes or wires that pass over fences or other perimeter barriers that may allow an adversary to pass over the barrier
- Tunnels, underpasses, culverts, or pipelines that pass under the perimeter barriers that are not adequately protected
- Adjacent structures in close proximity to either side of the fence that would facilitate bridging.

Buildings

E. Inspectors should determine whether construction materials are sufficient to provide appropriate delay against a number of adversary penetration methods, including hand tools, power tools, and explosives.

F. Inspectors should examine vaults to verify compliance with the construction requirements

specified in DOE Order 5632.1C and DOE Manual 5632.1C-1. Inspectors may accomplish this by visual examination and by looking at vault construction diagrams.

G. Inspectors should check safes, security cabinets, and other security containers to verify compliance with construction requirements specified in applicable DOE orders.

H. Inspectors should be prepared to conduct a thorough examination of a building. If only a portion of the building is a security area, the inspectors should be prepared to tour the security area perimeter, including areas that are within plenums and basements. It may be helpful to carry building floor plans. Other areas that should be checked include air ducts, electrical conduit and pipe penetrations, storage areas, and false ceilings.

I. Inspectors should review fixed barriers that protect protective force personnel (for example, towers, portals, alarm stations, and defensive positions) to determine whether they meet the requirements in DOE Order 5632.7A. Reviewing documents, interviewing security staff, or conducting visual inspections may accomplish this. A requirement that applies to posts constructed after 1985, designed to protect SNM (Category I or II), is that the exterior walls, windows, and doors must provide bullet resistance equivalent to the “high-power rifle” rating of UL 752. This can be checked by looking for a marking or stamp on the window or structure that indicates High-Power Rifle, HPR, or Level IV protection. Inspectors should also determine whether procedures are in place to preclude protective force personnel stationed within these posts from activities that could negate the purpose of these hardened posts.

J. Inspectors should review the design of vehicle barriers to determine whether they meet DOE standards (for example, to prevent entry of a 3,000-pound vehicle traveling at 50 miles per hour). This may require interviewing the responsible engineers, a review of vendor data, or a review of test results. Inspectors should also review barrier operational procedures to ensure that they are effectively integrated into the

protection strategy. Barriers left in the down position until identification of a potential threat or during a heightened security event do not prevent penetration by a malevolent vehicle during normal operations. Additionally, if credit is taken for emergency “up” operation of the barrier in the production strategy, testing should be performed to determine if the speed of activation of the barriers is adequate to counter the design basis threat.

K. Inspectors should review active denial systems to determine the effectiveness of their activation methods, and the conditions and procedures for activation. These systems should be examined to determine whether they are properly installed and in good condition, have effective power and power backup sources, and are tamper-resistant. The operator’s familiarity with system activation should also be checked.

Locks/Security Containers

L. Inspectors should review the key control system to determine whether procedures are in place to adequately control keys and locks. Typically, an effective key control system will include procedures that address control and accounting for keys and lock sets (this includes issue, signout, inventory, destruction, and the key and lock numbering system), and procedures used when a key is unaccounted for. Other factors that may be included are:

- Criteria for issuing a key or combination to a person (for example, supervisors developing authorized lists and notifying locksmiths in writing)
- Procedures to change lock combinations (for example, when a person possessing a combination transfers, resigns, is dismissed, or no longer requires access)
- Procedures and conditions for changing key locks or lock cores.

M. It may be helpful for inspectors to visit the lock shop or interview the locksmith to determine the adequacy of methods used for protecting

keying and core information. Other factors that should be considered are:

- The procedures for notifying the locksmith that locks or combinations need to be changed, and the time required to accomplish these changes. Inspectors may accomplish this by reviewing records. For example, when locks are changed because of a lost key, inspectors should be able to locate the records indicating when the key was reported lost, when the custodian reported the loss to the locksmith, when a work order was issued, and when the work was completed.
- The methods for numbering keys and locks, and whether the numbering methods unwittingly reveal information about the master-keyed system
- The procedures to periodically change combinations and lock cores
- The procedures to maintain locks, particularly locks that are exposed to severe weather conditions.

Delay Time

N. Inspectors should review documents, interview security staff, review as-built designs, and visually inspect barriers to determine the delay times the facility has estimated for various barriers. These estimates should be reviewed to determine whether they are credible, and whether protection is balanced (for example, a vault door used in a room with transite walls is a case of unbalanced protection, since one barrier is significantly more vulnerable than the other). Inspectors can also compare delay time estimates with response times and response procedures in order to determine whether response plans are effective and have been developed with appropriate consideration given to the physical security hardware.

Guidelines for identifying penetration times by reviewing site-specific documents are:

- SSSPs could conceivably contain parameters related to barrier delay times or to the

minimum delay times required to ensure an effective response. Such delay times may relate to individual components (such as doors) or to the total delay time involved in reaching a target or performing an action. However, most SSSPs do not provide this level of detail. Instead, they usually reference a site security plan or vulnerability assessment that may include delay time information.

- SSSPs may describe barriers, including doors and adjacent barriers. These descriptions may include penetration times for individual barriers or may reference the source of data used.
- VAs may contain penetration times for individual barriers in one or more locations. The narrative may address individual barriers and may include delay times. Also, computer codes are frequently used to conduct the VA. The input to these codes frequently includes delay times. For example, the Analytical System and Software for Evaluating Safeguards and Security codes are frequently used when developing VAs at DOE facilities. The input includes delay times for portal entry doors, exit doors, and surfaces. When reviewing computer input to determine the penetration times assumed by the facility, the following points should be considered:

- The input delay times may be different for different facilities or for different scenarios
- The input delay times may assume the door is secure, whereas there may be scenarios where the door is in access or is open
- If several barriers are in a series, the delay times may be added if the adversaries must pass all barriers to reach a target.

- System requirements documents or design specification documents are an excellent

source for determining expected penetration times. Unfortunately, such documents are not always available or are difficult to find. If these documents are available, the responsible security engineering group is the most likely source.

- Penetration times for doors and adjacent barriers can be significantly affected by a number of factors, including the mode and timing of the adversary attack and the adversary's level of sophistication.

Guidelines for visually inspecting barriers and reviewing as-built diagrams are:

- The construction and materials used in barriers can usually be determined by visual inspection or by a careful review of as-built diagrams. With this information, inspectors can generally make a rough estimate of penetration resistance. The Sandia barrier handbook, Non-proliferation and National Security Institute (formerly the Central Training Academy) Barrier Reference Guide, and other security design manuals may be useful for this purpose.
- During a visual inspection, the inspectors should focus on barrier deficiencies or design flaws that an outsider could exploit, allowing a surreptitious penetration of the barrier or a penetration in less time than estimated that an insider could exploit, allowing defeat of the protection element or allowing the insider to provide assistance to an outside force.

Guidelines for gathering information on penetration times by interviewing security staff or engineers are:

- Discussions with security personnel who conducted the VAs or who are responsible for barrier design may be useful for reviewing site-specific documents.
- If penetration times have been documented, the inspectors should interview knowledgeable security personnel in order to determine how penetration times were developed, what assumptions were made, what modes of

attack were considered, and what adversary threat characteristics were assumed.

- If penetration times have not been documented, the inspectors should interview knowledgeable security personnel in order to gather information on the effectiveness of the barrier design. Some of the potential discussion topics are:
 - Alarm response procedures (in particular, the sufficiency of response time in terms of barrier design)
 - Whether penetration resistance was factored into response plans
 - Design and construction (materials used, use of tamper-resistant hardware, hardening of barriers as part of an upgrade program).

General guidelines for using performance test results (conducted by OA-10 or others) to identify delay times are:

- OA-10 may conduct performance tests of barriers to determine penetration times. However, such tests frequently involve destructive techniques. It would be rare for OA-10 to conduct destructive tests of barriers for a variety of reasons, including safety concerns, cost of replacement, impact on operations and security, and the difficulty involved. In addition, tests involving a significant potential for personal injury (for example, crawling through razor ribbon) are not conducted.
- The types of tests for penetration times that inspectors would typically conduct would be simple ones designed to demonstrate potential vulnerabilities. For example, an inspector may conduct a simple test of an adversary's ability to defeat a steel-grate door that has a crash bar on the inside (such a test might involve using a bent rod and inserting it through the steel grate to engage the crash bar). These tests may demonstrate that the assumed delay times did not consider all credible modes of attack.

- OA-10 inspectors may identify penetration times by reviewing the results of tests on similar barriers that were conducted by the facility, other DOE elements, or outside agencies. Frequently, the facility has conducted (or contracted others to conduct) tests of barriers prior to their installation. Also, the vendors often have penetration time results for selected modes of attack. OA-10 may collect and review such information; however, test results should be critically reviewed. Particular attention should be paid to how the penetration times were determined, the modes of attack considered, the level of adversary sophistication, and the type of results reported.

Other general guidelines to be aware of when dealing with penetration times are:

- Penetration times are significantly influenced by the mode of attack. For example, hardened doors that would take several minutes to penetrate with power tools frequently can be breached via explosives in less than one minute. The inspection team should review the data and determine whether the modes of attack considered are consistent with the parameters of the approved threat guidance.
- Actions by a well-placed insider can defeat most barriers. For example, an insider can open a door from the inside and allow adversaries to enter, thus reducing the delay provided by the door. The inspection team should look for design features that would make a barrier particularly susceptible to defeat. The inspectors should also look for key insiders who are in a position to defeat multiple layers of protection. The inspection team should identify other protection measures in place to prevent insider tampering (for example, protective force patrols). The fact that well-placed insiders can defeat a barrier does not necessarily make that barrier inadequate, since multiple layers of protection should be afforded SNM. The potential actions of an insider need to be examined in a broader context, and considered in light of multiple layers of protection and parameters of the SSSP.
- There is inherent uncertainty associated with penetration time estimates; they are not precise values. Consequently, the comparison of penetration times is by its very nature a rough comparison. The intent is to determine whether the protection is reasonably balanced and whether the barriers provide sufficient delay to allow effective response. For example, if the penetration time of a door is 1.5 minutes, whereas the penetration time of the adjacent wall is two minutes, this will not normally be cause for concern (assuming the overall delay time is sufficient to allow effective response). However, if a Class 5 vault door is installed in a transite wall, this would clearly indicate unbalanced protection.