

## Section 3

## ENTRY AND SEARCH CONTROL

## Contents

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

## References

DOE Order 5632.1C  
DOE Manual 5632.1C-1

## General Information

Entry and search controls are established to prevent unauthorized access to security areas, removal of SNM, sabotage of vital equipment, and introduction of contraband. These controls may include access identification systems, search procedures, detectors, and barriers.

Security areas are established when the nature or importance of classified matter or security interests are such that access to them cannot be effectively controlled by other internal measures. Access to security areas is limited to persons who possess an appropriate clearance and who require access on a need-to-know basis. Access and search controls normally include a personnel identification system, positive verification of identity, a visitor log, inspection or search procedures, and signs indicating that trespassing is prohibited.

A security badge or pass system may be used to ensure that only authorized personnel enter, occupy, or leave a security area, and to indicate the limitations placed on access to classified matter. Badges, passes, and credentials are covered in detail in Section 4 of this guide.

Search systems range from physical and visual search procedures to the use of specialized

detection equipment, such as metal SNM and explosive detectors and x-ray machines. Since these systems are heavily dependent on personnel actions, inspectors must evaluate the training and capabilities of the individuals operating such equipment. Also, attention must be given to ensuring that search equipment is properly installed. The best-trained SPOs, using state-of-the-art equipment, cannot achieve the desired results if the equipment is not properly installed or maintained.

Subjects covered in this section are:

- CCTV identification systems
- Card-reader systems
- Biometric identifiers
- SNM detectors
- Metal detectors
- X-ray equipment.

A CCTV identification system may be used to provide positive identification of personnel entering security areas as an alternative to protection personnel stationed at the access control point to control access to a security area. CCTV systems allow remotely stationed protective personnel to view a person's face and identification badge. Equally effective access control measures must be in place whenever the CCTV identification system is inoperable.

Card readers and coded credentials may be used to supplement or replace badge checks as a means of access control. These devices are often used to control access to inner security areas and at

facility entry and exit portals. Door locks opened by card readers must be designed to relock after the door has closed to prevent a person from immediately opening the door while it is still in the unlock mode. Card readers at critical locations are usually provided with anti-passback protection. The coded credential technology includes a broad range of intricate applications, including bar codes, Weigand effect, magnetic stripe, proximity, and smart cards that will normally contain all information required for personal identification.

Biometric identifiers verify personal identity on the basis of some unique physical characteristic, such as eye-retinal pattern, hand geometry, voice, or fingerprints. Retinal scan and hand geometry devices are the most commonly used identifiers at DOE facilities. These devices may be used along with other controls, such as card readers or badge checks. Biometric identifiers are sophisticated devices that require proper installation, regular maintenance, and periodic servicing by authorized manufacturer's representatives.

SNM detectors usually include signal processing and annunciation equipment and are configured as portal, handheld, or vehicle devices. These detectors must be properly calibrated and sufficiently sensitive to meet site-specific protection objectives as defined in the SSSP.

Metal detectors may be used for searching personnel to ensure that explosive components, weapons, or other prohibited metal articles are not introduced without authorization. It is important that protective or other personnel are trained for clearing alarms and for taking appropriate actions if a violation is identified. Backup detectors (handheld) must be available at each location where metal detector portals are in use to resolve portal alarms and for use in the event of portal failure.

X-ray machines are also an acceptable means of searching many types of hand-carried items for concealed contraband or other unauthorized material. These machines must be capable of providing a clear picture of objects contained in packages or briefcases. Personnel operating the x-ray machines must be trained to recognize contraband, to take appropriate action when

suspect contraband is detected, and to operate the machine and recognize malfunctions.

## Common Deficiencies/ Potential Concerns

### Inadequate Monitoring

Inadequate monitoring results when SPOs are inattentive or cannot adequately view the search equipment (e.g., because of poor positioning or post design, or distraction by other duties). These conditions can allow the search equipment to be defeated, leading to unauthorized introduction or removal of material.

### CCTV Systems

There are a number of concerns when using CCTV identification systems. Since they may be vulnerable to disguise and false credentials, CCTV systems are usually not suitable for high-security areas such as an MAA. Also, inattention by protective force personnel is a common problem.

### Card-Reader Systems

A card-reader system does not verify the identity of a person; it identifies the coded badge or credential. For this reason, these systems are not acceptable as stand-alone systems for high-security areas, and require additional controls, such as badge checks, CCTV identification, or biometric identification. Coded credentials are also vulnerable to counterfeiting and decoding. If a lost or stolen badge is not voided in a timely manner, the potential for using the badge for unauthorized purposes increases. Additionally, if the authorized access lists are not updated frequently, the potential exists for persons who no longer have authorization to gain access to a restricted area.

### Biometric Identifiers

Facilities have had problems with biometric identifiers frequently rejecting authorized users. At these sites, alternative verification procedures that provide an acceptable level of identification must be available to avoid adverse impacts on the overall protection program. On the other hand,

some devices are too tolerant (for example, if the band of acceptance is too large, almost any hand, eye, or fingerprint will be accepted).

### SNM Detectors

SNM detectors are sensitive to the rate of speed at which individuals and vehicles pass through the detectors. For example, if an individual runs through the portal detector or items are thrown through, the detection probability can be substantially reduced. In any case, the SNM detector should be under visual surveillance when in use to prevent attempts to “pass around” or otherwise defeat the device.

### Metal Detectors

Metal that is passed through the detector very slowly or rapidly may avoid detection. For this reason, procedures are usually in place to monitor personnel and items passing through metal detectors. Individuals assigned to monitor this activity must be properly trained and be sufficiently diligent in order to recognize attempts to defeat metal detection devices. Inspectors should pay particular attention to testing of metal detectors at the floor level (in older detectors) due to the metal used in constructing the floor.

### X-Ray Equipment

X-ray equipment requires a close examination to ensure that the equipment is functioning properly to detect metal under required penetration depths, with sufficient resolution capability to effectively discern prohibited articles. The use of the standard step wedge with the requirement to image a 26-gauge wire at step five has not been uniformly implemented at all sites.

### Planning Activities

During inspection planning activities, inspectors interview points of contact and review available documents. Elements to cover include:

- General policies and criteria for access authorization at each security area. Potential criteria include:

- Personnel recognition
- Possession of a badge
- Possession of a badge and inclusion in a badge exchange system
- Enrollment in a coded credential system (e.g., card reader) and possession of a coded credential
- Enrollment in a biometric identification system
- Possession of a key
- Knowledge of a combination to a lock or keypad
- Knowledge of a code word.
- The method(s) (e.g., badge check, card reader, badge exchange) of verifying the identity of personnel entering each security area, including:
  - Property PA
  - LA
  - Exclusion area
  - SCIF
  - Secure communications center
  - Vital area
  - PA
  - MAA
  - Vault/vault-type room
  - Classified repository.
- Whether more than one method of access control is used at a security area (e.g., badge check and card reader), how the systems complement each other, and which is considered the primary means.

- General methods for determining a visitor's authorization and controlling access.
- Policies and procedures for vehicle control, including volume of traffic and the authorization process for private vehicles, government-owned vehicles, vendor vehicles, emergency vehicles, and SPO vehicles.
- General methods and procedures for conducting entry searches at each security area, especially each PA. (It should be noted that, absent dramatic improvement in technology, the only way that a vehicle can be effectively searched for weapons and/or explosives is by dismantlement of major components. Alternatively, vehicles may be escorted inside the protected area by the protective force.)
- General methods and procedures for conducting exit searches at each security area, especially each MAA.
- General information about each security area, including:
  - Normal operational hours (e.g., day shift Monday through Friday, or 24 hours a day and seven days a week)
  - Variations in normal operational hours
  - Approximate number of people assigned to the area
  - Approximate number of people with permanent access authorization to the area (including SPOs, fire squad, and other support groups)
  - Number of personnel portals and approximate throughput
  - Number of vehicle portals and approximate throughput.

## Performance Tests

Personnel Access Control Equipment (Appendix B, Part 1)

SNM Detectors (Appendix B, Part 2)

Metal Detectors (Appendix B, Part 3)

X-Ray Machines (Appendix B, Part 4)

Emergency Auxiliary Supplies (Appendix D, Part 1)

Tamper Protection (Appendix D, Part 2).

## Data-Collection Activities

### Policies and Procedures

**A.** Inspectors should determine whether there are policies in place that provide procedures on access control. These policies may cover personnel recognition, badge requirements, coded credentials and card readers, biometric identification systems, key control systems, combination lock or keypad requirements, or other access control measures.

**B.** Inspectors should determine whether there are policies and procedures for vehicle control, including private vehicles, government-owned vehicles, vendor vehicles, emergency vehicles, and SPO vehicles. Inspectors should determine which vehicles are authorized to enter security areas, how authorization is indicated (for example, sticker pass, government license plate), and how such indicators are requested, issued, and controlled. Inspectors should determine whether there are procedures in place to handle special or blanket authorizations for various types of vehicles, such as protective force, fire, maintenance, ambulance, and local law enforcement vehicles.

**C.** Inspectors should review protective force post orders, standard operating procedures, health physics policies, CAS procedures, and other relevant documents to determine whether they are complete, current, and consistent with site-specific policies.

**D.** Enrollment and de-enrollment procedures should be reviewed. This can be accomplished by asking the facility to print the enrollment list for one or more areas. Inspectors can verify the

names on the list by comparing the computer listing to other lists or by interviewing supervisors. Inspectors should determine if all persons on the list are authorized, if persons who recently transferred or terminated were removed in a timely manner, and if the lists are consistent with information available to SPOs at portals.

**E.** Inspectors should review search system policies, procedures, and calibration specifications for both personnel and vehicle searches; interview personnel who calibrate, test, and maintain search equipment and SPOs that monitor and respond to alarms; determine the length of time SPOs are required to operate detection equipment; tour areas where searches are conducted; and observe search procedures to determine whether searches are effective, whether detection equipment can be bypassed, and whether detectors and x-ray machines are properly calibrated. Inspectors should determine whether backup search equipment is available (for example, handheld metal and SNM detectors) and observe the conduct of searches with that equipment.

**F.** Inspectors should determine the access authorization policies and procedures for visitors, including cleared, uncleared, and foreign national visitors. Inspectors should review visit request initiation, processing, and approval, escort requirements, visitor identity verification, and visitor access authorization indication (for example, temporary badge, pass, photo identification, temporary card).

**G.** Inspectors should review automated entry control system policies to determine whether they are adequate. The review should include special features of the automated systems and the methods used to deter, detect, or prevent tampering.

**H.** Inspectors should determine whether individuals controlling access ensure that only persons with proper authorization are admitted and that positive verification of identity is established.

**I.** Inspectors should determine whether more than one method of access control is used at a security

area (for example, badge check and card reader), how the systems complement each other, and which is considered the primary means of access control. Similar to the intrusion-detection systems, these access systems should be complementary, not supplementary. A full understanding of the controls used may enable the inspectors to visualize potential problems and means to defeat the controls.

**J.** Inspectors should determine whether all vehicles, personnel, and hand-carried items entering and exiting PAs and MAAs are randomly searched, and whether the random search process is adequate. Inspectors should also determine whether all items belonging to uncleared personnel going in or out are inspected.

### Operations

**K.** Inspectors should observe operations at selected portals to verify compliance with site-specific procedures, including personnel and vehicle entry procedures, visitor controls, personnel and package searches, access logs, and the procedures used to place portals in access or secure mode. During observation of routine portal activities, it is prudent to request (in advance) that the test and maintenance personnel perform their normal testing and calibration activities.

**L.** Inspectors should observe operations at selected storage areas, including vaults, vault-type rooms, safes, or other storage areas. Inspectors should check entry procedures to include requests to put alarm systems in access mode, lock and double-lock systems, entry logs, interfaces with protective force or health physics, control methods in the access mode (such as CCTV, SPO posted at door, two-person rule, and lock-up procedures, including exit searches, lock checks, and procedures to place the alarm system in secure mode). All of these procedures should be reviewed in light of the possibility of a single insider gaining access to SNM or other security interest. The controls should be structured in such a way that DOE interests are not at risk from a single insider.

**M.** Except in the case of an emergency response, protective force personnel should not normally be exempt from the requirements for personnel entering certain security areas. Even though protective force personnel are allowed to take authorized weapons and other duty equipment

into a security area, they should not be exempt from routine access controls. Such exemption would be an ideal opportunity for the introduction of contraband or unauthorized material into a security area.