

APPENDIX B
ACCESS CONTROL SYSTEM
PERFORMANCE TESTS

Part 1: Personnel Access Control Equipment	B-1
CCTV Identification System	B-7
Card-Reader Systems	B-12
Biometric Identifiers	B-19
Part 2: SNM Detectors	B-27
SNM Detector—Walk-Through Testing	B-33
SNM Detector—Vehicle Monitor	B-39
SNM Detector—Handheld	B-45
Part 3: Metal Detectors	B-51
Metal Detector—Walk-Through	B-56
Metal Detector—Handheld	B-62
Part 4: X-Ray Equipment—Package Searches	B-67

Part 1

Personnel Access Control Equipment

Objective	B-1
System Tested	B-2
Scenario	B-2
Evaluation	B-3
Assessing Equipment Performance	B-4
Interpreting Results	B-4
Special Considerations	B-5
Responsibilities	B-5
Internal Coordination	B-5
Security Considerations	B-5
Personnel Assignments	B-5
Logistical Requirements	B-5
CCTV Identification System	B-7
Checklist—CCTV Identification System—Access Control Equipment	B-9
Card-Reader Systems	B-12
Checklist—Card-Reader Systems—Access Control Equipment	B-15
Biometric Identifiers	B-19
Checklist—Biometric Identifiers —Access Control Equipment	B-22

Part 1

Personnel Access Control Equipment

Objective

The objective is to test the effectiveness of equipment (that is, card readers, remote CCTV identification hardware, and biometric systems) used to control access to security areas or used to supplement other access controls (for example, badge checks).

DOE orders require that only authorized personnel be allowed to access security areas. Also, the identification of personnel entering a PA, MAA, or LA must be verified. The use of devices such as card readers and biometric or CCTV identification systems is not mandatory; such devices may be used to complement SPO badge checks or as a stand-alone system. (At PAs, SPOs must administer the access controls. This requirement has generally been interpreted to mean that the use of unattended access control systems at PAs is prohibited.) For facilities that use access control hardware, the most directly applicable DOE requirements are:

Applicability**Order Reference**

PA

DOE Manual 5632.1C-1,
Chapter V, Paragraph 5

MAA

DOE Manual 5632.1C-1,
Chapter V, Paragraph 7

Vital Area

DOE Manual 5632.1C-1,
Chapter V, Paragraph 6

CASs (Category I or II SNM Facilities)

DOE Manual 5632.1C-1,
Chapter V, Paragraph 8b
and c

LA

DOE Manual 5632.1C-1,
Chapter V, Paragraph 3

Exclusion Area

DOE Manual 5632.1C-1,
Chapter V, Paragraph 4

Secure Communications Centers

DOE Manual 5632.1C-1,
Chapter V, Paragraph 8e

SCIFs	DOE Manual 5632.1C-1, Chapter V, Paragraph 8a
CASs (Classified Matter Facilities)	DOE Manual 5632.1C-1, Chapter V, Paragraph 8b
Government Property and Unclassified Facilities	DOE Manual 5632.1C-1, Chapter V, Paragraph 2
CCTV ID Systems	See requirements for each security area
Card Readers	See requirements for each security area
Biometric	See requirements for each security area

System Tested

System	- Access control system
Functional Element	- Personnel authorization, identification, and verification
Component(s)	- Card readers, CCTV identification systems, biometric identifiers (for example, hand geometry, retinal scans, voice recognition), transmission lines, access control central processing equipment, and interfaces with CCTV and CAS operation; testing and maintenance of access control equipment

Scenario

Inspectors should select one or more security area portals for testing. The selection is based on the consideration of a number of factors, including portal configuration and location, operating history, number of portals, type of security areas where access control devices are used, and the type of devices used (for example, card reader, biometric system, CCTV). Inspectors should look for potential deficiencies or misapplication of technology. Before testing the devices, the inspectors should clearly understand how the access control systems function and what features are used at each portal. The inspectors should observe the facility's security alarm technicians or SPOs as they conduct routine operational and sensitivity testing of selected devices. Inspectors should select devices for testing based on the number, type, configuration, deployment, and operational history. When observing the testing of devices, inspectors should note the procedures used to determine whether test and maintenance procedures are consistent with DOE orders and approved SSSPs, and whether they are an effective means of testing the systems.

Inspectors accomplish two goals by having the facility's security technicians conduct routine testing. First, these tests indicate the effectiveness of the facility test and maintenance program. Inspectors can observe the test procedures to determine whether they are effective and, at the same time, determine whether the tested devices are operational. Second, facility testing should verify that devices are functional according to facility specifications; thus there is assurance that the inspectors will be testing a system that is operating as the facility intends. This may be important in identifying the root cause of deficiencies.

If all features of the devices are not tested by the facility, the inspectors may conduct their own testing, as appropriate. The purpose of the testing is to determine whether the devices function as intended and whether an adversary could exploit design or operational deficiencies and gain access to a security area without proper authorization.

The inspectors should monitor the annunciation in the CAS, SAS, or at the portal, depending on the system design. The inspectors can also observe the operation of interfacing systems, including automatic CCTV display, video recorders, and the CAS operators.

The number of portals and devices selected for testing depends on the time available, the importance of the system in the overall protection program, and the variation in individual portals. The following guidelines are intended to assist inspectors in selecting sensors and zones for testing:

- Test at least two portals. If the portals use different types of devices, or if the device configuration at each portal is significantly different, inspectors should consider selecting at least one of each type.
- Test at least one of each type of device (if the devices are used for protecting high-priority targets, such as Category I quantities of SNM).
- If the first few tests do not indicate problems and there is no evidence of exploitable deficiencies, the inspectors should not devote extensive time to testing numerous other portals or devices. However, if deficiencies exist, inspectors should collect sufficient data to determine whether the deficiencies represent isolated problems or whether they are systemic.
- Inspectors should conduct tests at portals in which deficiencies were noted on initial tours. For example, inspectors may note that there are no apparent means of verifying that only one person at a time enters an unattended LA portal where card readers are used to control access; in such cases, the inspectors should conduct tests to determine whether this situation could be exploited by an adversary.

Evaluation

For the access control system to be effective, the combination of hardware and procedural controls must be sufficient to prevent unauthorized entry to security areas. This section deals primarily with evaluating the access control devices; specifically card readers, biometric identifiers, and CCTV identification systems. Included are guidelines for assessing device performance and interpreting results in the context of system performance.

Assessing Equipment Performance

The primary objective in evaluating an access control device is to determine whether the device effectively and reliably discriminates between authorized and unauthorized access attempts, and whether it denies unauthorized access. Other questions that should be asked are:

- Is the device a stand-alone system or is it used in conjunction with a badge check or another means of access control?
- Are there provisions for visually monitoring (either directly or by CCTV) the portals where access control devices are used?
- Will an alarm be initiated if the portal door is forced open or opened from the inside in an unauthorized manner, and where does it report?
- Can the portal be bypassed (for example, climb over the portal into the security area) without creating an alarm condition?
- Will power outages cause equipment failures that will impact security?
- Will an alarm condition be annunciated if a person is denied access authorization after a specified number of access attempts?
- Are there provisions to prevent piggybacking or unauthorized use of another person's credentials?

Interpreting Results

The following guidelines are provided to assist inspectors in interpreting results:

- An access control system usually consists of multiple layers. Each layer is only as good as its weakest link. Tests that indicate that a knowledgeable adversary could enter the security area without authorization or detection through one or more portals are evidence that the access controls are not effective. The significance of this deficiency must be analyzed in the context of the site-specific protection objectives and the effectiveness of complementary systems.
- In some cases, tests indicate that a device can be defeated but that, because of the degree of redundancy in the portal configuration, an adversary entering the security area would also have to defeat multiple security devices or other controls (for example, a badge check). In such cases, the identified deficiencies are less serious because of the defense-in-depth employed. However, the deficiencies may indicate design or testing and maintenance problems.
- Facility tests may indicate the system is functional even though inspector testing indicates the devices can be defeated. In such cases, the inspector can reasonably conclude there are deficiencies in the test procedures or the quality assurance program.
- Facility tests indicating that devices are functional, in conjunction with inspector tests confirming that the devices are effective, are evidence that the tested portions of the system are effective and test and maintenance procedures are also effective. However, the limitations of the tests must be recognized. For example, not all modes of defeat (for example, piggy-backing) may have been fully tested.

Special Considerations

Related tests or activities, such as testing of search equipment or communications equipment, are typically conducted concurrently with the testing of devices.

Responsibilities

Inspectors: Select the portals and devices. Direct tests and monitor alarm annunciation. (Typically one inspector will be stationed at the CAS and at least one at the portal.)

Facility: Conduct routine tests. Provide security technicians. Provide test devices as necessary (for example, coded cards for card-reader tests), and provide SPOs for security during tests as required. Provide radios for two-way communication.

Internal Coordination

Testing of devices should be scheduled to avoid conflicts with other tests involving the protective force.

Security Considerations

Observe all normal security considerations. Normally, an SPO must monitor (directly or by CCTV) tests to ensure that no unauthorized personnel enter the PA.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Security technicians

Equipment:

- Radios
- Test devices

Safety:

- Follow normal operating procedures
- Complete a safety plan
- Notify the CAS and other alarm monitoring stations before testing is conducted
- Station one inspector in the CAS
- Arrange to prevent any undesired protective force armed response to alarms

CCTV Identification System

System Description:	CCTV systems are used to verify the identity of personnel entering a security area. Such systems allow a remotely stationed SPO to conduct a badge check by simultaneously viewing images of a person and his badge. Alternatively, the SPO may compare a person's image to a stored video image.
Components of CCTV ID Systems:	Camera, transmission lines, monitor, remote door lock activator, electric door lock

Concerns

- In most cases, CCTV identification systems do not include provisions for searching personnel and are not suitable for portals where searches are required.
- If SPOs do not pay adequate attention to verifying identity, unauthorized personnel may be allowed entry.
- Remote CCTV identification systems are vulnerable to persons disguising their faces or using false or stolen credentials. As such, they are not suitable for high-security purposes (for example, MAAs or PAs); however, CCTV identification may be adequate for compartmentalizing areas within a security area.
- Uneven lighting, shutdown, glare, or degraded equipment may drastically reduce the capability to effectively compare images.
- If the CCTV identification system (or related controls) does not include provisions for preventing “tailgating” or “piggy-backing” (two or more persons entering an area using only one credential), the facility may be vulnerable to insiders deliberately allowing access, or employees unwittingly allowing access, to unauthorized persons. Measures to deter tailgating include having SPOs monitor the area or using mantraps (interlocked doors or turnstiles designed to ensure that only one person passes through at a time).
- Cameras and related systems and monitors require periodic maintenance to ensure reliable operation.
- Systems without uninterruptible or auxiliary power will not operate in the event of a power failure. Facilities with systems that fail in the non-secure mode (for example, electric locks that fail in the open position) may be vulnerable to unauthorized access during periods when power is unavailable because of natural events, accidents, or deliberate sabotage.

Types of Tests

- Electric Door Lock Tests

One test involves verifying that the door lock engages immediately after the door closes so that a person following immediately behind cannot open the door before the door lock engages. The inspectors should examine the door and electric lock system to determine whether it can be defeated by techniques such as blocking the lock operation or cutting power to magnetic locks.

- Door Alarm Interface Tests

These tests are conducted to determine whether the door alarm is operational and integrated with the remote control. One such test is to hold the door open for an extended period (that is, 30 seconds or more) to determine whether an alarm condition is initiated. This test is usually applicable only at unattended doors.

- Visual Inspection of CCTV Monitor

The inspectors should enter the CAS, SAS, or other location where a CCTV identification monitor is located and observe image quality. If any CCTV identification portals are outdoors, observation of monitors under day and night conditions is recommended.

Test Guidelines

- The most frequent problem with CCTVs is improperly maintained equipment. The inspectors should visually check the quality of the images on the monitors at the CAS, SAS, and other control locations.
- Tests of electric door locks or door alarm interfaces should be conducted at portals that are used for high-security application and are not protected by other means (for example, SPOs stationed at the post who can monitor the entrance).
- Tests involving unauthorized personnel or persons using improper credentials may be designed to test the alertness of the SPOs who monitor the CCTV identification system. However, such tests must be conducted without the knowledge of the SPO and require detailed safety plans.

Checklist

CCTV Identification System

Access Control Equipment

Interview Items

Installation location _____

Maintenance frequency and procedure _____

Type of lock controlled by card reader (if any) _____

Enrollment procedures (video comparator only) _____

De-enrollment procedure (video comparator only) _____

Alternative means of granting access _____

Tour/Visual Inspection Items

Environmental protection _____

SPO capability to monitor door and passageway _____

Mantrap or turnstile configuration _____

Door lock configuration _____

Door alarm configuration _____

Quality of image in monitor _____

**Data Collection Sheet
CCTV Identification System**

Test Method

	Zone Tested	Zone Number	ID System	ID Confirmation Method	Electric Door Locks	Door Alarm Interface	Special Features
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
Comments:							

Card-Reader Systems

System Description:	Card readers and coded credentials are used to supplement or replace badge checks as a means of access control. The coded credential may be a separate card or it may be imbedded in a photograph identification badge. The coded credential may be used alone or in conjunction with a biometric device or a Personnel Identification Number (PIN). The card reader may be used to operate electric locks, to provide information to an SPO at the post, or to do both.
Coded Credential Technologies:	Optical Bar code Magnetic – spot Magnetic – stripe Weigand effect Proximity Capacitance Smart cards
Components of Card Reader:	Card reader, electric lock, coded credential, central controller, printer, enrollment console, PIN keypads, transmission lines, multiplexors, tamper indicators (switches or line supervision)
Features of Card Reader Systems (not all systems have all features):	Time zone Area zone Anti-passback Occupant listing Fail soft Operator manual override

Concerns

- By itself, a card-reader system does not verify the identity of a person. Card-reader systems are not acceptable as stand-alone systems for high-security applications, including PAs, MAAs, and LAs. Additional controls such as badge checks, remote CCTV identification, or biometric identification are necessary to verify that the person who possesses a coded credential is authorized to enter an area. Stand-alone card-reader systems may be an acceptable means of controlling access to rooms or areas within a larger security area in an effort to enhance security by compartmentalization.
- Most coded credentials can be decoded or counterfeited by using the appropriate equipment and information. If credentials are lost, stolen, compromised, or not voided (that is, deleted from the system) in a timely manner, the potential for adversaries to use such credentials increases. Also, adversaries may obtain a credential from an authorized person by force, stealth, deceit, or through the voluntary or coerced assistance of an insider.

- If the card-reader system (or related controls) does not include provisions for preventing tailgating (two or more persons entering an area using only one credential), the facility may be vulnerable to insiders deliberately allowing access, or employees unwittingly allowing access, to unauthorized persons. Measures to deter tailgating include having SPOs monitor the area or using mantraps (arrangements of interlocked doors or turnstiles designed to ensure that only one person passes through at a time).
- If the card-reader system (or related controls) does not include provisions for preventing passback (for example, an authorized person enters an area and passes his card back to another person, who then enters the area), the facility may be vulnerable to insider actions. Measures to deter passback include mantraps, effective lane control, monitoring by SPOs, and anti-passback features associated with the card-reader system.
- Card readers require periodic maintenance to ensure reliable operation. Card readers located outdoors require more frequent maintenance.
- Card readers that do not have a means of detecting tampering (for example, tamper switches and line supervision or continuous SPO monitoring) may be susceptible to defeat.
- If the authorized access lists are not reviewed and updated frequently (by deleting the credentials), the potential exists for persons who no longer have a need to access the area to enter that area. Similarly, if there is a lag time between the time when a person is no longer permitted access (for example, the individual is reassigned or terminated) and the time his access credentials are actually deleted (de-enrollment), a window of vulnerability exists.
- Systems without uninterruptible or auxiliary power will not be operational in the event of a power failure. Facilities with systems that fail in the non-secure mode (for example, electric locks that fail in the open position) may be vulnerable to unauthorized access during power outages (due to natural events, accidents, or deliberate sabotage).
- Facilities that have enrollment procedures that do not include provisions for verifying the enrollment request may be vulnerable to unauthorized enrollment.
- Facilities having enrollment procedures that do not ensure that only authorized personnel enroll or delete credentials, or do not include provisions for supervisory approval (or other procedures to verify only proper credentials are enrolled), may be vulnerable to the employees (particularly those who operate the enrollment system) acting as insiders.
- PINs may be compromised if PIN keypads are not designed to prevent bystanders from observing the PIN entry.
- Fail-soft features (operation in a degraded mode with a lower level of security) may degrade access controls if other hardware or procedural controls are not used in conjunction with the badge reader.

Types of Tests

- **Improper Card Tests**

These tests are conducted to verify that access is not allowed (for example, door is not opened) when an invalid card is used. Repeated failures to access should result in an alarm for those systems equipped to detect repeated, unsuccessful access attempts.

- Tamper Alarm Tests

In these tests, card readers, multiplexors, or junction boxes are opened to test tamper switches. Alarm wires are shorted to test line supervision. Testing should be conducted in both access and secure modes if the entrance is so configured.

- Electric Door Lock Tests

One test involves verifying that the door lock engages immediately after the door closes so that a person following immediately behind cannot open the door before the door lock engages. Inspectors may also examine the door and electric lock system to determine whether it can be defeated by techniques such as blocking the lock operation or cutting power to magnetic locks. This test is only applicable at unattended doors that are controlled by card-reader systems.

- Door Alarm Interface Tests

These tests are conducted to determine whether the door alarm is operational and integrated with the card-reader control. One such test is to simply hold the door open for an extended period (for example, 30 seconds or more) and determine whether an alarm condition is annunciated. This test is usually only applicable at unattended doors.

- Special Features Tests

Special features, such as time zoning or anti-passback capability, must be tested. Inspectors should attempt to use a card in a manner that should not result in access being granted. For example, the inspector can enter an MAA, exit that MAA without reading out, attempt to enter the MAA again (or attempt to enter a second MAA), and verify that access is denied or an alarm condition initiated.

Test Guidelines

- Card-reader systems tend to operate reliably and rarely fail in a non-secure mode if designed properly. The tests are conducted primarily to verify information about system capabilities or features. As such, a small number of tests are usually sufficient. Testing that involves an improper card and testing of tamper alarms should be performed at two or three portals.
- Special features, if required, may be tested as appropriate for the site-specific system. Such testing requires the inspector to understand the system's features and how they are implemented (for example, the card readers at an MAA entrance may use different features than those at a PA entrance or a different MAA).
- Problems most frequently encountered with card-reader systems are those involving the interface with the door lock or alarm. Testing of door locks or door alarm interfaces should be conducted at portals that are used for high-security application and are not protected by other means (for example, SPOs stationed at the post who can monitor the entrance).

Checklist

Card-Reader Systems

Access Control Equipment

Interview Items

Installation location _____

Operational test frequency and method _____

Maintenance frequency and procedure _____

False alarm history/records _____

Tamper alarm (switches or line supervision) _____

Mode of operation (stand-alone or as a supplement to SPOs) at different locations _____

Technology of coded credential (for example, bar code) _____

Use with PIN or biometric device _____

Type of lock controlled by card reader (if any) _____

Enrollment procedures _____

De-enrollment procedure (lag time) _____

Card-Reader Systems

Time zoning _____

Area zoning _____

Anti-passback _____

Occupant listing _____

Fail-soft _____

Operator manual override _____

Visual Inspection Items

Environmental protection _____

SPO capability to monitor door and passageway _____

Mantrap or turnstile configuration _____

Door lock configuration _____

Door alarm configuration _____

**Data Collection Sheet
Card-Reader Systems**

Test Method

	Zone Tested	Zone Number	Card Type	Improper Card	Tamper	Electric Door Lock	Door Alarm Interface	Special Features
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
Comments:								

Biometric Identifiers

System Description: Biometric devices are used to verify identity based on some unique physical characteristic of the individual. Biometric devices may be used as a stand-alone system or in conjunction with other controls, such as card readers, PINs, or badge checks. The biometric device may be used to operate electric locks, provide information to an SPO, or do both.

Biometric Technologies: Voice verification
Eye-retinal pattern verifier
Fingerprint verifier
Hand geometry

Components of Biometric ID Systems (not all systems have all features) Biometric device, electric lock, central controller, printer, enrollment console/device, PIN keypads, transmission lines, multiplexors, tamper (switches and line supervision)

Features of Biometric Time zone Device Systems (not all systems have features) Area zone
Fail-soft
Occupant listing
Operator manual override

Concerns

- Biometric devices are used at only a few DOE facilities. Retinal scan and hand geometry devices are the most commonly used. If properly applied, the use of biometric devices can be a significant strength.
- Some facilities have problems with their devices frequently rejecting authorized users. Alternative verification procedures that provide an acceptable level of security should be available to avoid unacceptable impacts on operations.
- Some types of devices can be fooled, if repeated attempts are allowed. The system should be designed to detect successive rejections that may indicate an imposter is attempting to match a biometric template. Provisions should also be made to monitor the portal directly or by CCTV to minimize the potential for tampering with the system or using a fabricated or forged biometric sample.
- If the biometric device system (or related controls) does not include provisions for preventing tailgating (two or more persons entering an area using only one credential), the facility may be vulnerable to insiders deliberately allowing access, or employees unwittingly allowing access, to unauthorized persons. Measures to deter tailgating include having SPOs monitor the area or using mantraps (arrangements of interlocked doors or turnstiles designed to ensure that only one person passes through at a time).
- Biometric devices require periodic maintenance to ensure reliable operation.

- Biometric devices that do not have a means of detecting tampering (for example, tamper switches and line supervision or continuous SPO monitoring) may be susceptible to defeat.
- If the authorized access lists are not reviewed and updated frequently (by deleting the person's authorization), the potential exists for persons who no longer have a need to access the area to enter that area. Similarly, if there is a lag time between the time when a person is no longer permitted access and the time his access credentials are actually deleted (de-enrollment), a window of vulnerability exists.
- Systems without uninterruptible or auxiliary power will not be operational in the event of a power failure. Facilities with systems that fail in the non-secure mode (for example, electric locks that fail in the open position) may be vulnerable to unauthorized access during power outages (due to natural events, accidents, or deliberate sabotage).
- Facilities that have enrollment procedures that do not include provisions for verifying the enrollment request may be vulnerable to unauthorized enrollment.
- Facilities having enrollment procedures that do not ensure that only authorized personnel enroll or delete credentials, or do not include provisions for supervisory approval (or other procedures to verify that only proper credentials are enrolled), may be vulnerable to employees (particularly, those who operate the enrollment system) acting as insiders.
- PINs may be compromised if PIN keypads are not designed to prevent bystanders from observing the PIN entry.
- Fail-soft features (operation in a degraded mode with a lower level of security) may degrade access controls if other hardware or procedural controls are not used in conjunction with the badge reader.

Types of Tests

- Attempted Entry by Unauthorized Person

This test is conducted to verify that an unauthorized person who attempts to enter is not allowed access. Repeated access attempt failures should result in an alarm for those systems equipped to detect repeated, unsuccessful access attempts.

- Tamper Alarm Tests

In these tests, biometric devices, multiplexors, or junction boxes are opened to test tamper switches. Alarm wires are shorted and opened to test line supervision. Testing should be conducted in both access and secure modes if the portal is so configured.

- Electric Door Lock Tests

One test involves verifying the door lock engages immediately after the door closes so that a person following immediately behind cannot open the door before the door lock engages. The inspectors may also examine the door and electric lock system to determine whether it can be defeated by techniques

such as blocking the lock operation or cutting power to magnetic locks. This test is only applicable at unattended doors that are controlled by card-reader systems.

- **Door Alarm Interface Tests**

These tests are conducted to determine whether the door alarm is operational and integrated with the card-reader control. One such test is to simply hold the door open for an extended period (that is, 30 seconds or more) and determine whether an alarm condition is initiated. This test is usually only applicable at unattended doors.

- **Special Features Tests**

Special features, such as time zoning or anti-passback capability, must be tested. Inspectors should attempt entry in a manner that should not result in access being granted. For example, inspectors should enter an MAA, exit that MAA without reading out, attempt to enter the MAA again (or attempt to enter a second MAA), and verify that access is denied or an alarm condition initiated.

Test Guidelines

- Biometric device systems tend to operate reliably and rarely fail in a non-secure mode if designed properly. The tests are conducted primarily to verify information about system capabilities or features. Thus, a small number of tests are usually sufficient. Tests involving attempted entry by an unauthorized person and tests of tamper alarms should be performed at two or three portals.
- Special features, if required, may be tested as appropriate for the site-specific system. Such testing requires the inspector to understand the system's features and how they are implemented (for example, the biometric devices at one MAA entrance may use different features than those at a second MAA).
- Problems most frequently encountered with biometric systems are those involving the interface with the door lock or alarm. Testing of electric door locks or door alarm interfaces should be conducted at portals that are used for high-security applications and are not protected by other means (for example, SPOs stationed at the post who can monitor the entrance).

Checklist

Biometric Identifiers

Access Control Equipment

Interview Items

Installation location _____

Operational test frequency and method _____

Maintenance frequency and procedure _____

False alarm history/records _____

Tamper alarm (switches or line supervision) _____

Mode of operation (stand-alone or as a supplement to SPOs) at different locations _____

Technology (for example, retinal scan) _____

Used with PIN or card reader _____

Type of lock controlled by biometric device system _____

Enrollment procedures _____

De-enrollment procedure (log time) _____

Biometric Device System Features

Time zoning _____

Area zoning _____

Occupant listing _____

Fail-soft _____

Operator manual override _____

Visual Inspection Items

Environmental protection _____

SPO capability to monitor door and passageway _____

Mantrap or turnstile configuration _____

Door lock configuration _____

Door alarm configuration _____

Data Collection Sheet
Biometric Identifiers

Test Method

	Zone Tested	Zone Number	Biometric Identifier	Unauthorized Entry	Tamper Alarm	Electric Door Lock	Door Alarm Interface	Special Features
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
Comments:								

This page is intentionally left blank.

Part 2

SNM Detectors

Objective	B-27
System Tested	B-27
Scenario	B-27
Evaluation	B-28
Interpreting Results	B-29
Special Considerations	B-30
Responsibilities	B-30
Internal Coordination	B-30
Security Considerations	B-31
Personnel Assignments	B-31
Logistical Requirements	B-31
Definitions	B-31
SNM Detector—Walk-Through Testing	B-33
Checklist—SNM Detector—Walk-Through	B-36
SNM Detector—Vehicle Monitor	B-39
Checklist—SNM Detector—Vehicle Monitor	B-42
SNM Detector—Handheld	B-45
Checklist—SNM Detector—Handheld	B-47

Part 2

SNM Detectors

Objective

The objective of these limited scope performance tests is to determine the effectiveness of SNM detectors to detect the unauthorized removal of SNM through an access control portal. The most directly applicable requirements are:

Applicability**Order Reference**

Category I and II SNM

DOE Manual 5632.1C-1,
Chapter V, Paragraph 5

Category I and II SNM, MAAs

DOE Manual 5632.1C-1,
Chapter V, Paragraph 7

Category I and II SNM

DOE Manual 474.1-1,
Chapter III, Paragraph 5d**System Tested**

System - Access control system

Functional Element - Exit search

Component(s) - Detectors (handheld, portal, vehicle), including signal processing equipment and annunciation equipment; testing and maintenance of detectors

Scenario

The inspectors should select one or more SNM detectors for testing. This selection is based on consideration of a number of factors, including portal configuration and location, operating history, the number of portals, the different types of SNM detectors in use (vehicle, walk-through, handheld), and the types of locations where SNM detectors are used (PAs, MAAs, others).

The inspectors should then observe the facility's security alarm technicians or SPOs as they conduct the routine operational or sensitivity tests of selected SNM detectors. During this portion of the test, the inspectors should observe the test procedures used in order to determine whether the tests, calibrations, and maintenance procedures are consistent with DOE orders, approved SSSPs, and whether they are an effective means of testing the systems.

Two goals are accomplished by having the facility's security technicians conduct routine testing prior to testing by inspectors. First, the facility tests indicate the effectiveness of the test and maintenance program.

Inspectors can observe the test procedures to determine whether they are effective and have an opportunity to determine whether the selected SNM detectors are properly calibrated. Second, the facility's tests should verify that the detectors are calibrated according to facility specifications; thus, there is assurance that the inspectors will be testing a system that is operating as the facility intends. This may be important in identifying the root cause of deficiencies.

The inspectors should then conduct operational and sensitivity testing as appropriate for the type of detectors in use. The purpose of these tests is to determine whether the detectors are properly calibrated and whether they are sensitive enough to meet site-specific protection objectives.

The number of detectors selected for testing depends upon the time available, the importance of the system in the overall protection program, and the variation in the types of detectors used at different portals. The following guidelines are intended to assist the inspector in selecting detectors for testing:

- At very small facilities, or at facilities with only a few (that is, less than five) SNM portals, the inspectors may elect to test detectors at each portal. At larger facilities, the inspectors would typically select two to four portals for testing.
- Because of the configuration of the security layers, at many facilities the exit searches at the MAAs are more critical for protecting SNM than those at PAs or outer security areas. Consequently, in many cases, it is appropriate to focus efforts on the SNM detectors at MAA portals. However, SNM detectors at PA portals should not normally be completely neglected.
- Normally, the inspectors should test at least one of each type of detector (that is, handheld, vehicle, walk-through). However, the inspectors need not test each type of detector at each portal selected.
- If the first few tests do not indicate problems and there is no evidence of exploitable deficiencies, the inspectors should not generally devote extensive time to testing numerous additional detectors. However, if deficiencies are apparent, the inspectors should collect sufficient data (by testing additional detectors) to determine whether a deficiency is an isolated instance or evidence of a systemic problem. Also, if testing indicates that detectors are not sufficiently sensitive to detect the goal quantity of SNM, the inspectors may elect to repeat testing with larger sources (if available) to determine the magnitude of the deficiency.

Evaluation

If exit searches are to be effective, the SNM detection equipment must be part of an integrated system consisting of hardware, personnel, and procedures. This section deals primarily with the evaluation of the SNM detector hardware. Guidance is provided on assessing detection effectiveness and on interpreting results in the context of system performance.

The primary objective in evaluating an SNM detector is to determine whether the unit effectively and reliably detects the passage of a determined quantity of SNM through the detection zone. Other points that should be considered in the evaluation are:

- Are there provisions for monitoring personnel, packages, or vehicles passing through the detection zone in order to ensure that normal procedures are followed? For example, are there provisions for ensuring that personnel:

- do not bypass the detector zone?
 - do not throw items through the detection zone?
 - do not pass through walk-through monitors at an unusually high rate of speed (that is, run instead of walk)?
 - do not pass items through walk-through monitors at an extremely slow speed?
 - do not drive through vehicle detector zones at an unusually high speed?
 - do follow all site-specific procedures?
- Is the system of barriers and procedures at the SNM portal sufficient to ensure that material is not passed around the detector?
 - Are there adequate provisions for detecting shielded SNM (that is, metal detectors used in conjunction with SNM detectors)?
 - Are the SPOs who monitor the SNM detectors trained in using the equipment, and are they familiar with the search procedures?
 - Are SNM detector alarm response procedures clear, complete, and sufficient to ensure that all anomalies are resolved prior to allowing egress?
 - Are provisions adequate to ensure that unauthorized personnel do not tamper with the SNM detection equipment and do not have access to control settings?
 - Do the detectors have features, such as high- and low-background alarms, that alert the protective force to conditions that could alter detection capability? If not, are alternate measures in place to provide adequate assurance?
 - Are testing and maintenance procedures sufficient to provide assurance that the detectors are reliable and correctly calibrated?
 - Have the test sources been selected with appropriate consideration of the type and form of SNM in the security area?
 - Do the test procedures include all aspects of detector operation, including tests of high-background alarms, low-background alarms, and occupancy sensor operation?
 - If plutonium sources are used for testing, are there provisions to ensure that only low burn-up Pu test sources are used?

Interpreting Results

The following guidelines are provided to assist the inspectors in interpreting results in the context of system performance.

- Testing that indicates that the SNM detectors can be bypassed or do not reliably detect removal of significant quantities of SNM (that is, significantly greater than the goal quantity) is evidence of a potentially serious deficiency. The significance of such deficiencies must be analyzed in the context of site-specific protection objectives and the effectiveness of other complementary systems. In general, deficiencies in SNM detectors at a portal are most significant at facilities that have Category I or II quantities of SNM in portable forms and that rely on a single layer of exit search. Potential factors that may partially mitigate deficiencies in SNM detection equipment are additional layers of exit searches; material controls that provide high assurance that material is not diverted; and SNM in forms (for example, large pieces or irradiated) that are less likely to be successfully diverted.
- Testing that indicates a slight miscalibration or detector drift is significant, but much less serious than gross miscalibrations or exploitable deficiencies. For example, testing may indicate the goal quantity (for example, 10 grams U-235) could be passed through the detector at shoe level eight out of ten tries at one facility portal. Additional testing may indicate a slightly larger test source (for example, 15 grams U-235) could be reliably detected (for example, ten out of ten passes). Such results would indicate a miscalibrated sensor, but not a serious vulnerability. However, these results also indicate a possible testing and maintenance deficiency, and the inspectors should consider conducting additional tests in order to determine whether the miscalibration is an isolated case or a systemic problem.

Special Considerations

OA-10 inspectors do not possess any radioactive test sources and must use test sources provided by the facility. The inspectors should contact the facility point of contact early in the planning process to determine what types and sizes of test sources are available.

It is preferable to test SNM detectors by using the type of SNM that is located within the security area (for example, plutonium sources in plutonium processing areas and uranium sources in uranium processing areas). Occasionally, the facility will conduct testing and calibration activities using a different type of source (for example, barium or cesium) and will not have a uranium or plutonium source. In such cases, inspectors should determine whether a standard uranium or plutonium source can be obtained or whether small quantities of the SNM used in the facility's process lines can be used to test the detectors.

Related testing and activities, such as metal detector tests and reviews of portal barriers and procedures, are typically conducted concurrently with SNM detector testing to increase the efficiency of data gathering.

Responsibilities

Inspectors: Select the portals and detectors. Direct testing and monitor alarm annunciation.

Facility: Conduct routine tests. Provide test sources. Assign SPOs to provide security during testing, as required. Provide security technicians to conduct testing at the direction of the inspectors.

Internal Coordination

Testing should be scheduled to avoid conflicts with other tests involving the protective force. Testing should be coordinated with the MC&A topic team (if any) to avoid duplication of effort.

Security Considerations

Observe all normal security considerations. Normally, a protective force representative must monitor testing to ensure that security is maintained.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Alarm technicians

Equipment:

- Test sources
- Shielding material (as needed)

Safety:

- Follow normal operating procedures
- Complete a safety plan
- Notify the CAS and other alarm monitoring stations before testing
- Station one inspector in the CAS
- Inspectors should arrange to prevent any undesired, armed responses to alarms by the protective force

Definitions

Facility technicians use calibration test sources to calibrate detectors and to perform acceptance testing. For walk-through monitors these sources are typically ten grams U-235 or one gram plutonium. The calibration procedures typically call for the calibration source to be passed through the detector at normal walking speed at selected locations. The acceptance criterion is 50 percent detection probability with 95 percent confidence, although some facilities use a more stringent criterion for calibration purposes.

Detection zone is the area for which the detectors are designed to effectively detect SNM. For walk-through or vehicle detectors, the detection zone is the area between the detectors. For handheld detectors, this is the area exposed to the detector during the search procedures.

Goal quantity is the quantity of SNM that is to be reliably detected when passed through the detection zone.

This may be defined on a site-specific basis with DOE field element approval. Traditionally, standard test sources are ten grams U-235 or one gram plutonium, which should be detected anywhere in the detection zone with 50 percent detection probability at 95 percent confidence when the source is passed through the detector at normal walking speed. The inspectors should assume these test sources are the goal quantity unless the facility has identified, justified, and documented an alternative site-specific goal quantity in an approved SSSP. A goal quantity defined by a facility would typically be larger than the calibration source.

The larger goal quantity may be justified on the basis of the type of SNM in the security area (that is, no bulk material or small pieces) or in consideration of the other material controls and detection mechanisms that would make it unlikely that an adversary could remove a large quantity of SNM (that is, Category I or II) from a security area by diverting small amounts of SNM (less than a goal quantity) over an extended period in a large number of attempts (for example, if the goal quantity is 20 grams of U-235, it would take 250 diversions of 20 grams to accumulate a Category I quantity of uranium metal).

SNM Detector—Walk-Through Testing

Typical Uses

- To detect SNM at MAA personnel egress points
- To detect SNM at PA personnel egress points

Concerns

- Personnel are typically in the detection zone of a portal monitor for only a short time, and detection capability is sensitive to the rate of speed at which they pass through the detectors. The detectors are typically calibrated and tested with a test source carried by a person who walks through the detector at a normal rate of speed. If the speed of exiting personnel is not adequately controlled (that is, if personnel are not prevented from running or throwing items through the detectors), the detection capability can be substantially reduced.
- Detectors, wiring, and electronics may be susceptible to tampering if they are not adequately protected by methods such as buried lines, locked control panels, or tamper alarms.

Types of Tests

- Operability Tests

These tests are conducted to verify proper operability of the detector. They simply involve walking through the detection zone with a goal quantity of SNM or the standard test source according to the normal procedures at that post (which may include requirements for a short pause before proceeding). Such testing should be conducted with the source placed near the left edge, center, and right edge of the detection zone and at different elevations (for example, shoe level, waist level, head level).

- Sensitivity Tests

Sensitivity tests are conducted to determine whether the detector is correctly calibrated. Such testing generally involve observing a security technician as he conducts the acceptance test that would normally be conducted after a calibration.

This may involve a series of walk-throughs designed to demonstrate that the detector has an acceptable detection probability.

- High-Background Tests

High-background tests are conducted to verify that high-background alarms operate as designed. Generally, the facility's or manufacturer's test procedures are followed. Testing typically involves slowly moving a radiation source toward the SNM detector (without setting off the occupancy sensor) while monitoring the detector count rate in order to verify the high-background alarm occurs at the specified threshold value.

- Low-Background Tests

Low-background tests are conducted to verify low-background alarms operate as designed. Generally, the facility's or manufacturer's test procedures are followed. Testing typically involves disabling or shielding the detectors to reduce the count rate. The inspectors monitor the count rate to verify the alarm occurs at the specified threshold.

- Occupancy Sensor Tests

SNM detectors use a variety of occupancy sensors to detect the presence of personnel and to initiate the monitoring measurement. The most commonly used sensors include photoelectric, ultrasonic, microwave, infrared, and pressure sensitive. Occupancy sensors are tested to verify sensor operability. Generally, the facility's or manufacturer's test procedures are followed and typically involve entering the detection zone and verifying the alarm.

- SNM Detection Capability Tests

Inspectors may elect to conduct additional testing of detection sensitivity, focusing on the capability of the detectors to detect SNM removal. Such testing may involve using SNM in the form and quantity found in the security area and testing the detection capability with the SNM concealed at various locations on the body, or in packages. The inspectors should use their knowledge of SNM detectors, occupancy detectors, and search procedures to conduct tests that will challenge the system. For example, inspectors can attempt to pass material through the walk-through monitor while avoiding the occupancy sensor. Another example is a "kick test," which involves placing the SNM at shoe level and swinging the foot through the detector as fast as possible when walking through (minimizing the time in the detection zone). Testing should be conducted with a quantity of SNM that is equal to or greater than the goal quantity.

- Shielded SNM Tests

Inspectors may elect to conduct testing of the detector's capability to detect shielded SNM. Such tests involve shielding SNM with lead or other shielding material. Inspectors can then determine the amount of shielding that is necessary to prevent detection of a significant quantity of SNM (for example, a Category I quantity). It is recognized that any quantity of SNM can be shielded and detection prevented if a sufficient amount of shielding is used. Shielding tests can be used to determine how much shielding would be necessary. Such information can be used to determine whether the other search procedures (for example, visual observation as the person passes through the portal) are a credible means of detection, and can also be used as a baseline for performance tests of SPO search procedures. For example, if shielding tests indicate that a 20-pound lead container will prevent detection of a Category I quantity of SNM, then the inspectors might conduct testing of the SPO's visual search procedures involving a lead container in a toolbox.

Test Guidelines

- Typically, the inspectors conduct operability tests, sensitivity tests, high-background tests, low-background tests, and occupancy sensor tests at a few key portals (typically two or three). If the facility has a large number of portals and those portals use several different types of detectors or substantially different search procedures, then the inspectors may choose to test one of each major type of portal detector.

- SNM detection capability tests and shielded SNM tests should be conducted at a typical portal if an appropriate SNM source and shielding is available. Frequently, such tests require extensive security precautions, particularly if Category II or greater quantities of SNM are involved. The inspectors may, instead, elect to review the results of similar tests or analyses conducted by the facility to determine the capability to detect SNM in shielded or unshielded configurations.
- If any deficiencies are noted in the installation or operation of detectors, or in the implementation of search procedures, the inspectors should conduct testing to exploit those deficiencies in order to determine their significance/extent. For example, if the inspectors note that a SNM walk-through detector is not adequately monitored by SPOs, then the inspectors could design and conduct tests to determine whether a person could successfully throw a significant quantity of SNM through the detector in an attempt to avoid detection. Additional tests could be conducted to determine how large a quantity could be diverted by that method. Tests that are designed to indicate whether the SPO notes any unusual behavior (for example, throwing items through the detector) might be considered.
- If an individual detector can be defeated, that same detector should be tested again to determine whether such defeat is repeatable. Several tests of the same detector may be required to determine whether an adversary can exploit a deficiency.
- If an individual SNM detector can be defeated by one or more methods (for example, walk-through, pass around), the similar SNM detectors at other portals should be tested by the same method in order to determine the extent of the problem. If possible, inspectors should conduct several (three to five) more tests at different portals. If most of these tests indicate the detector can be reliably defeated, there is sufficient evidence a systemic problem exists. If no other detectors are defeated, then one may conclude that an isolated deficiency was identified. If the results are inconclusive, the inspector should consider testing more detectors. Rarely would an inspector test more than five detectors by the same method.
- If the adversary has sufficient knowledge, time, and equipment, all SNM detectors can be defeated by using sufficient quantities of shielding. Testing should generally be conducted only if a portal is particularly vulnerable (for example, due to lack of metal detection capability) or if direct visual observation CCTV or SPOs at posts are considered inadequate to provide reasonable assurance that such attempts can be detected.

Checklist
SNM Detector
Walk-Through

Interview Items

Installation location _____

Operational test frequency _____

Operational test method _____

Sensitivity test frequency _____

Sensitivity test method _____

False alarm history/records _____

Make/model _____

Tamper protection _____

Provisions for personnel with medical conditions that cause alarms _____

Tour/Visual Inspection Items

Control settings protected? _____

Occupancy sensor? _____

SPO monitoring method (CCTV, direct)? _____

One-way or two-way traffic? _____

Metal detector used? _____

Package search method? _____

**Data Collection Sheet
SNM Detector – Walk-Through Monitors**

Test Method

	Zone Tested	Portal Location	Operability	Sensitivity	Kick	High Background	Low Background	Occupancy Sensor	Detection	Shielded SNM	Other
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
Comments:											

SNM Detector—Vehicle Monitor

Typical Uses

- To detect SNM at MAA vehicular egress points
- To detect SNM at PA vehicular egress points
- To detect SNM at key roadways or badge check stations

Types

- Portal Monitors—drive through during monitoring
- Monitoring Station—vehicle stationary during monitoring
- Handheld—various types

Concerns

- Vehicles are typically in the detection zone of a portal monitor for only a short time, and detection capability is sensitive to the rate of speed at which they pass through the detectors. The detectors are typically calibrated and tested with a test source in a vehicle that is moving through the detector at a normal rate of speed. If the speed of exiting vehicles is not adequately controlled (that is, if the vehicles are allowed to pass through the monitors at a rate significantly faster than that used for calibration), the detection capability can be reduced.
- Highly effective vehicle searches are difficult to achieve. Vehicle monitors are typically less sensitive than personnel monitors because of the greater distances between detectors. Further, vehicles are constructed from radiation-attenuating material and are capable of transporting large masses of shielding material. Facilities must attempt to strictly limit vehicular access to areas that have significant quantities of SNM. Also, failure to conduct a visual inspection, concurrent with the vehicle monitor search, reduces the assurance that attempts to divert shielded SNM will be detected.
- Portal monitors are typically installed in housings six to eight feet tall. Large trucks can be considerably taller than the portal monitors. The capability to detect SNM concealed near the top of all vehicles may be reduced if no supplemental measures (such as visual searches or searches with handheld detectors) are enacted for tall vehicles.
- Detectors, wiring, and electronics may be susceptible to tampering if they are not adequately protected by methods such as buried lines, locked control panels, or tamper alarms.

Types of Tests

- Operability Tests

These tests are conducted to verify proper operability of the detector. They simply involve driving (or walking, assuming the vehicle occupancy detector can be activated) through the detection zone with a

goal quantity of SNM or the standard test source. These tests should be conducted with the source placed near the left edge, center, and right edge of the detection zone.

- Sensitivity Tests

Sensitivity tests are conducted to determine whether the detector is correctly calibrated. Such tests generally involve observing a security technician as he conducts the acceptance test that would normally be conducted after a calibration. This may involve a series of pass-throughs designed to demonstrate that the detector has an acceptable detection probability.

- High-Background Tests

High-background tests are conducted to verify that high-background alarms operate as designed. Generally, the facility's or manufacturer's test procedures are followed. Testing typically involves slowly moving a radiation source toward the SNM detector (without setting off the occupancy sensor) while monitoring the detector count rate in order to verify that the high-background alarm occurs at the specified threshold value.

- Low-Background Tests

Low-background tests are conducted to verify that low-background alarms operate as designed. Generally, the facility's or manufacturer's test procedures are followed. Testing typically involves disabling or shielding the detectors to reduce the count rate. The inspectors monitor the count rate to verify that the alarm occurs at the specified threshold.

- Occupancy Sensor Tests

SNM detectors use a variety of occupancy sensors to detect the presence of vehicles and to initiate the monitoring measurement. The sensors commonly used include photoelectric, microwave, infrared, pressure-sensitive, and metal detectors. Occupancy sensors are tested to verify sensor operability. Generally, the facility's or manufacturer's test procedures are followed. These typically involve entering the detection zone and verifying the alarm.

- SNM Detection Tests

Inspectors may elect to conduct additional tests of detection sensitivity, focusing on the capability of the detectors to detect SNM removal. Such tests may involve using SNM in the form and quantity found in the security area and testing the detection capability with the SNM concealed at various locations on the vehicle (for example, in the trunk, on the roof, or under the hood). The inspectors should use their knowledge of SNM detectors, occupancy detectors, and search procedures to conduct testing that will challenge the system. For example, inspectors can attempt to minimize the time the SNM is in the detection zone by placing the source near the front of the vehicle and driving through the detectors as fast as practical (while maintaining safety). Testing should be conducted with a quantity of SNM equal to or greater than the goal quantity.

- Shielded SNM Tests

Inspectors may elect to conduct tests of the detector's capability to detect shielded SNM. Such tests involve shielding SNM (in the form and quantity in the security area) with lead or other shielding material. Inspectors can then determine the amount of shielding that is necessary to prevent detection

of a significant quantity of SNM (for example, a Category I quantity). It is recognized that any quantity of SNM can be shielded and detection prevented if a sufficient amount of shielding is used. Shielding tests can be used to determine how much shielding would be necessary. Such information can be used to determine whether the other search procedures (for example, visual searches) are a credible means of detecting removal attempts, and can also be used as a baseline for performance tests of SPO search procedures. For example, if shielding tests indicate that a 100-pound lead container will prevent detection of a Category I quantity of SNM, then the inspectors might consider conducting tests of the SPO's visual search procedures involving a "suspicious" 100-pound lead container in a vehicle.

Test Guidelines

- Typically, the inspectors conduct operability tests, sensitivity tests, high-background tests, low-background tests, and occupancy sensor tests at a few key portals (typically two or three). If the facility has a large number of vehicle portals and those portals use several different types of detectors or substantially different search procedures, then the inspectors may choose to test one of each major type of vehicle portal detector.
- SNM detection capability tests or shielded SNM tests should be conducted at a typical portal if an appropriate SNM source or shielding is available. Frequently, such tests require extensive security precautions, particularly if Category II or greater quantities of SNM are involved. The inspectors may instead elect to review the results of similar tests or analyses conducted by the facility to determine the capability to detect SNM in shielded or unshielded configurations.
- If any deficiencies are noted in the installation or operation of detectors, or in the implementation of search procedures, the inspectors should conduct tests that exploit those deficiencies in order to determine their significance. For example, if the inspectors note that an occupancy sensor is configured such that a small vehicle might exit the portal without tripping the occupancy sensor, then the inspectors could design and conduct testing to determine whether a vehicle carrying SNM could exploit the situation and avoid detection. Additional testing could be conducted to determine how large a quantity could be diverted by that method, and other tests might be considered that are designed to indicate whether the SPO notes that a vehicle is attempting to drive through the portal in an unusual pattern (that is, attempting to avoid the occupancy sensor).
- If an individual detector can be defeated, that same detector should be tested again to determine whether such defeat is repeatable. Several tests of the same detector may be required to determine whether an adversary can reliably exploit a deficiency.
- If an individual SNM detector can be defeated by one or more methods (for example, walk-through, pass around), then similar SNM detectors at other portals should be tested by the same method in order to determine the extent of the problem. If possible, inspectors should conduct several (three to five) more tests at different portals. If most of these tests indicate the detector can be reliably defeated, there is sufficient evidence to conclude that a systemic problem exists. If no other detectors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, the inspector should consider testing additional detectors. Rarely would an inspector test more than five detectors by the same method.
- If the adversary has sufficient knowledge, time, and equipment, all SNM detectors can be defeated by using sufficient quantities of shielding. Such testing should generally be conducted only if a portal is particularly vulnerable (for example, due to lack of visual searches).

Checklist

SNM Detector

Vehicle Monitor

Interview Items

Installation location _____

Operational test frequency _____

Operational test method _____

Sensitivity test frequency _____

Sensitivity test method _____

False alarm history/records _____

Make/model _____

Tamper protection _____

Tour/Visual Inspection Items

Separation between detector posts? _____

Control settings protected? _____

Alarm lines buried? _____

Occupancy sensor? _____

Vehicle trap or single gate? _____

Visual search conducted? _____

One-way or two-way traffic? _____

**Data Collection Sheet
SNM Detector – Vehicle**

Test Method

	Zone Tested	Operability	Sensitivity	Kick	High Background	Low Background	Occupancy Sensor	Detection	Shielded SNM	Other
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										

Comments:

SNM Detector—Handheld

Typical Uses

- To detect SNM at MAA personnel egress points
- To detect SNM at PA personnel egress points
- To investigate anomalies at portals where walk-through detectors are normally used
- To use as backups if walk-through or vehicle detectors fail
- To conduct vehicle searches
- To search at vault exits
- To search at non-routine doors
- To search packages and hand-carried items.

Concerns

- Handheld detectors can be brought very close to areas where SNM could be concealed, and thus have the potential for detecting very small quantities of SNM. However, the effectiveness of the search is highly dependent on the diligence of the SPOs who conduct the searches. If the SPO does not search personnel thoroughly (back and front, both sides) or does not take sufficient time, the detection probability can be significantly reduced.
- At portals where traffic is high or when several persons exit at once, SPOs may be rushed or have difficulty controlling (separating) personnel.
- Proper operation of the detectors is essential for an effective search. SPO training is also essential to ensure that they can operate the equipment. SPOs should know how to properly orient the detector for the most effective searches. Sufficient space is necessary to properly use the detectors and to ensure continuity of operations.
- Handheld detectors may be susceptible to tampering if not adequately controlled.
- Handheld detectors operate on batteries and require regular maintenance.

Types of Tests

- Operability Tests

These tests are conducted to verify proper operability. They generally involve placing SNM or other radiation sources near the detector, observing the count rate, and verifying an alarm condition.

- Sensitivity Tests

Sensitivity tests are conducted to verify proper detection sensitivity. Such tests generally involve observing an SPO or security technician during conduct of routine acceptance tests. These tests generally involve placing a specific radiation source at a specified distance, monitoring the count rate, and verifying an alarm condition.

- Shielding or Other SNM Detection Capability Tests

Other tests involving shielded material or SNM concealed in a vehicle or on personnel can be conducted as described in this performance test.

Test Guidelines

- Typically, the inspectors conduct operability tests and sensitivity tests at a few key portals (typically two or three).
- SNM detection capability tests and shielded SNM tests should be conducted at a typical portal if an appropriate SNM source or shielding is available. Frequently, such tests require extensive security precautions, particularly if Category II or greater quantities of SNM are involved. The inspectors may, instead, elect to review the results of similar tests or analyses conducted by the facility to determine the capability to detect SNM in shielded or unshielded configurations.
- If any deficiencies are noted in the installation or operation of detectors, or in the implementation of search procedures, the inspectors should conduct testing to exploit those deficiencies in order to determine the significance. For example, if the inspectors note that the SPOs do not usually search the backsides of personnel, then the inspectors could design and conduct tests to determine whether a person carrying SNM in his back pocket could exploit the situation and avoid detection.
- If an individual detector can be defeated or does not have proper sensitivity, that same detector should be tested again to determine whether such defeat is repeatable. Several tests of the same detector may be required to determine whether an adversary can exploit the deficiency.
- If an individual SNM detector can be defeated or does not have proper sensitivity, the similar SNM detectors at other portals should be tested by the same method in order to determine the extent of the problem. If possible, the inspectors should conduct several (three to five) more tests at different portals. If most of these tests indicate that the detector can be reliably defeated, there is sufficient evidence that a systemic problem exists. If no other detectors are defeated, then one may conclude an isolated deficiency was identified. If the results are inconclusive, the inspectors should consider testing additional detectors. Rarely would an inspector test more than five detectors using the same method.
- If the adversary has sufficient knowledge, time, and equipment, all SNM detectors can be defeated by using sufficient quantities of shielding. Tests should generally be conducted only if a portal is particularly vulnerable (for example, due to poorly implemented search procedures).

Checklist
SNM Detector
Handheld

Interview Items

Location of use _____

How used (backup, normal search, anomaly investigation) _____

Operational test frequency _____

Operational test method _____

Sensitivity test frequency _____

Sensitivity test method _____

Make/model _____

Storage when not in use _____

Tour/Visual Inspection Items

Storage location? _____

Used according to procedure? _____

Means of traffic control? _____

**Data Collection Sheet
SNM Detector – Handheld**

Test Method

	Zone Tested	Portal Location	Operability	Sensitivity	Shielding or Other SNM Detection Capability
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

This page is intentionally left blank.

Part 3

Metal Detectors

Objective	B-51
System Tested	B-51
Scenario	B-51
Evaluation	B-52
Interpreting Results	B-53
Special Considerations	B-54
Responsibilities	B-54
Internal Coordination	B-54
Security Considerations	B-54
Personnel Assignments	B-55
Logistical Requirements	B-55
Definitions	B-55
Metal Detector—Walk-Through	B-56
Checklist—Metal Detector—Walk-Through	B-59
Metal Detector—Handheld	B-62
Checklist—Metal Detector—Handheld	B-64

Part 3

Metal Detectors

Objective

The objective is to test the effectiveness of metal detectors at detecting unauthorized introduction of metallic contraband, or removal of metallic SNM/shielding, through an access control portal. Although metal detectors may be used at facilities that do not possess SNM, they are primarily used at SNM facilities. The most directly applicable requirements are:

Applicability

Category I and II SNM or Vital Equipment,
PA Entrance

Category I and II SNM PA Exits

Category I and II SNM, MAAs

Category I and II SNM MC&A

Order Reference

DOE Manual 5632.1C-1,
Chapter V, Paragraph 5

DOE Manual 5632.1C-1,
Chapter V, Paragraph 5

DOE Manual 5632.1C-1,
Chapter V, Paragraph 7

DOE Manual 474.1-1,
Chapter III, Paragraph 5d

System Tested

System - Access control system

Functional Element - Entry and exit searches

Component(s) - Detectors (handheld, walk-through), including signal processing equipment and annunciation equipment; testing and maintenance of detectors

Scenario

The inspectors should select one or more metal detectors for testing. The selection is based on consideration of a number of factors, including portal configuration and location, operating history, the number of portals, the different types of metal detectors in use (walk-through, handheld), and the types of locations where metal detectors are used (PAs, MAAs, others).

Inspectors should observe the facility's security alarm technicians or SPOs conducting the routine operational or sensitivity testing of selected metal detectors. During this portion of the test, the inspectors

should observe the test procedures to determine whether the tests, calibrations, and maintenance activities are consistent with DOE orders and approved SSSPs and whether they are an effective means of testing the systems. The inspector accomplishes two goals by having the facility's security technicians conduct these routine tests. First, the facility's tests indicate the effectiveness of the test and maintenance program. The inspector can determine whether they are effective and can also have an opportunity to determine whether the selected metal detectors are properly calibrated. Second, the facility's tests should verify that the detectors are calibrated according to facility specifications; thus, there is assurance that inspectors will be testing a system that is operating as the facility intends. This may be important in identifying the root cause of deficiencies.

Inspectors should then conduct operational and sensitivity tests, as appropriate. The purpose of these tests is to determine whether the detectors are properly calibrated and whether they are sufficiently sensitive to meet site-specific protection objectives.

The number of detectors selected for testing depends on the time available, the importance of the system in the overall protection program, and the variation in the types of detectors used at different portals. The following guidelines are intended to assist the inspector in selecting detectors for testing:

- At very small facilities, or at facilities with only a few (that is, less than five PA or MAA portals), the inspectors may elect to test detectors at each portal. At larger facilities, the inspectors would typically select two to four portals for testing.
- Because of the configuration of the security layers, at many facilities the exit searches at the MAAs are more critical for protecting SNM than those at PAs or outer security areas. Consequently, in many cases, it is appropriate to focus efforts on the metal shielding detectors at MAA portals. However, the metal shielding detectors at PA portal exits should not normally be completely neglected.
- Entry searches at PA portals are required by DOE orders. Some facilities conduct searches at MAA exits in addition to the PA entry searches. A few facilities conduct entry searches at MAA entrances in lieu of those at PA entrances; this requires an approved exception to DOE orders. Inspectors should determine where entry searches are conducted and focus their efforts on the locations that are more critical from a security perspective.
- If the first few tests do not indicate problems and there is no evidence of exploitable deficiencies, the inspectors should not generally devote extensive time to testing numerous additional detectors. However, if deficiencies are apparent, the inspectors should collect sufficient data (by testing additional detectors) to determine whether a deficiency is an isolated instance or there is evidence of a systemic problem. Also, if tests indicate detectors are not sufficiently sensitive to detect the goal quantity of metal, inspectors may elect to repeat tests with larger items (if available) to determine the magnitude of the deficiency.

Evaluation

In order for exit searches to be effective, the metal-detection equipment must be part of an integrated system consisting of hardware, personnel, and procedures. This section deals primarily with the evaluation of the metal-detector hardware. Guidance is provided on assessing detection effectiveness and interpreting results.

The primary objective in evaluating the metal detector is to determine whether the unit effectively and reliably detects the passage of metallic weapons or specified goal quantities of shielding through the detection zone. Other points that should be considered in the evaluation are:

- Are there provisions for monitoring personnel, packages, or vehicles passing through the detection zone in order to ensure that normal procedures are followed? For example, are there provisions for ensuring that personnel:
 - do not bypass the detector zone?
 - do not throw items through the detection zone?
 - do not pass through walk-through monitors at an unusually high rate of speed (for example, run instead of walk)?
 - pause while in walk-through detectors?
 - do not pass items through walk-through monitors at an extremely slow speed?
 - follow all site-specific procedures?
- Is the system of barriers and procedures at the portal sufficient to ensure material is not passed around the detector?
- Are the SPOs who monitor the metal detectors trained in using the equipment, and are they familiar with the search procedures?
- Are metal detector alarm response procedures clear, complete, and sufficient to ensure that all anomalies are resolved before allowing ingress or egress?
- Are provisions adequate to ensure that unauthorized personnel do not tamper with the metal detection equipment and do not have access to control settings?
- Are testing and maintenance procedures sufficient to assure that the metal detectors are reliable and correctly calibrated?

Interpreting Results

The following guidelines are provided to assist the inspectors in interpreting results in the context of system performance.

- Testing that indicates that the metal detectors can be bypassed or do not reliably detect the passage of metallic weapons or the goal quantity of metallic shielding is evidence of a potentially serious deficiency. The significance of such deficiencies must be analyzed in the context of site-specific protection objectives and the effectiveness of other complementary systems. In general, deficiencies in metal-shielding detectors (at exits) at an MAA portal are most significant at facilities that have Category I or II quantities of SNM in portable forms and that rely on a single layer of exit search. Deficiencies in metal detectors used to detect contraband (at entrances) lead to the potential for adversaries to bring weapons into a security area. Potential factors that may partially mitigate

deficiencies in metal-detection equipment are additional layers of exit searches (for example, at the MAA and PA); material controls that provide high assurance that material is not diverted; and SNM in forms (that is, large pieces or irradiated) less likely to be successfully diverted.

- Testing that indicates a slight miscalibration or detector drift is significant but much less serious than gross miscalibrations or exploitable deficiencies. For example, tests may indicate the goal quantity of shielding material (for example, 100 grams of aluminum) could be passed through the detector at shoe level eight out of ten tries at one facility portal. Additional tests may indicate that a slightly larger test quantity (for example, 150 grams of aluminum) could be reliably detected (for example, ten out of ten passes). Such results would indicate a miscalibrated sensor, but not necessarily a serious vulnerability. However, these results may indicate a testing and maintenance deficiency, and inspectors should consider conducting additional tests to determine whether the miscalibration is an isolated case or a systemic problem.

Special Considerations

If the inspectors use test weapons or items provided by the facility, the facility point of contact should be contacted early in the planning process to determine what types and sizes of metal objects or test weapons are available.

Related tests and activities, such as SNM detector tests and reviews of portal barriers and procedures, are typically conducted concurrently with metal-detector tests.

Responsibilities

Inspectors: Select the portals and detectors. Direct testing and monitor alarm annunciation.

Facility: Conduct routine tests. Provide test sources. Assign SPOs to provide security during tests, as required. Provide security technicians to conduct testing at the direction of the inspectors.

Internal Coordination

Testing should be scheduled to avoid conflicts with other tests involving the protective force. Tests of metal shielding detectors should be coordinated with the MC&A topic team (if any) to avoid duplication of effort.

Security Considerations

All normal security considerations should be observed. Normally, a protective force representative must monitor tests to ensure that security is maintained.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel

- Protective force representative
- Alarm technicians

Equipment

- Test weapons (disabled)
- Shielding material simulator, ferrous and non-ferrous

Safety

- Follow normal operating procedures
- Complete a safety plan
- Notify the CAS and other alarm monitoring stations before any testing
- Station one inspector in the CAS
- Inspectors should arrange to prevent any undesired armed responses to alarms by the protective force

Definitions

Detection zone is the volume at which the detectors are designed to effectively detect metal. For walk-through detectors, this is the area between the detectors. For handheld detectors, this is the area exposed to the detector during the search procedures.

Goal quantity is the quantity of metal that is to be reliably detected when passed through the detection zone; this may be defined on a site-specific basis with DOE field element approval. Standard quantities should be considered to be 100 grams of ferrous or non-ferrous metal for shielding, and 200 grams of ferrous or non-ferrous metal for weapons. These quantities should be used as a goal quantity unless the facility has identified, justified, and documented an alternative goal quantity in an approved SSSP.

Metal Detector—Walk-Through

Typical Uses

- To detect SNM/shielding on personnel at MAA or PA personnel egress points (in conjunction with SNM detectors)
- To detect metallic weapons on personnel at PA (and possibly MAA) personnel ingress points

Types

- Pulsed field
- Continuous wave

Concerns

- Commercial metal detectors detect only moving metal. Metal objects transferred through a detector very slowly may not be detected. For effective searches, procedures must be in place to monitor personnel passing through the detection zone to ensure that no unusual activity occurs (such as very slow movement).
- Many facilities require workers to wear safety shoes that are generally steel-toed. These steel-toed shoes are a common source of nuisance alarms. Some facilities will desensitize their detectors at shoe level; however, this practice is not acceptable from a security perspective.
- The sensitivity of metal detectors can be impacted by nearby metal structures, such as swinging metal doors or metal in walls or floors. Typically, it is desirable to locate metal detectors three or more feet away from massive metal structures.
- The sensitivity of metal detectors is not uniform. The position of the metal object in the detection volume and the orientation of the object can greatly affect detection sensitivity. Test procedures should test detection capability for a variety of locations and orientations.
- Metal detectors that are calibrated to detect 100 grams of non-ferrous metal are extremely sensitive and are likely to alarm when a wide variety of common objects (belt buckles, eyeglasses, coins) are passed through or when nearby metal objects are moved (for example, a swinging door). To operate effectively, high-sensitivity detectors must be located carefully (away from metal structures and, perhaps, away from other screening equipment such as x-ray units and monitors), provided with surge-free electric power, and maintained in a temperature-controlled environment. Also, provisions must be made to examine hand-carried or personal items.
- To ensure effective searches, provisions must be made for searching personnel who set off metal detectors with metal surgical implants or metal dental work.
- Detectors, wiring, and electronics may be susceptible to tampering if they are not adequately protected by methods such as buried lines, locked control panels, or tamper alarms.

Types of Tests

- Operability Tests

These tests are conducted to verify proper operability of the detector. They simply involve walking through the detection zone with a metal object (weapon, test object, or goal quantity of shielding). Such tests should be conducted with the source placed near the left edge, center, and right edge of the detection zone and at different elevations (for example, shoe level, waist level, head level).

- Sensitivity Tests

Sensitivity tests are conducted to determine whether the detector is correctly calibrated. Such testing generally involves observing a security technician during conduct of the acceptance test that would normally be conducted after a calibration. This may involve a series of walk-throughs designed to demonstrate that the detector has an acceptable detection probability.

- Occupancy Sensor Tests

Although not common, some metal detectors use occupancy sensors to detect the presence of personnel in order to reduce false alarms. The sensors may be photoelectric, ultrasonic, microwave, infrared, and pressure sensitive. Occupancy sensors are tested to verify sensor operability. Generally, the facility's or manufacturer's test procedures are followed and typically involve entering the detection zone and verifying the alarm.

- Metal Detection Capability Tests

Inspectors may elect to conduct additional testing of detection sensitivity, focusing on the capability of the detectors to detect passage of metal. Such testing may involve using weapons or goal quantities of shielding and testing the detection capability with the metal concealed at various locations on the body or in packages. The inspectors should use their knowledge of metal detectors, occupancy detectors, and search procedures to conduct testing to challenge the system. For example, inspectors can attempt to pass material through the walk-through monitor while avoiding the occupancy sensor. Another example is a "kick test," which involves placing the weapon/shielding at shoe level and swinging the foot through the detector as fast as possible when walking through (minimizing the time in the detection zone). Tests should be conducted with a disabled weapon or quantity of shielding equal to or greater than the goal quantity.

Test Guidelines

- Typically, the inspectors would conduct operability tests, sensitivity tests, and other appropriate tests (such as kick tests) at a few key portals (typically two or three). If the facility has a large number of portals and those portals use several different types of detectors or substantially different search procedures, then the inspectors may choose to test one of each major type of portal detector.
- If any deficiencies are noted in the installation or operation of detectors, or in the implementation of search procedures, the inspectors should conduct tests that exploit those deficiencies in order to determine their significance. For example, if the inspectors note a walk-through metal detector is not adequately monitored by SPOs, the inspectors could design and conduct testing to determine whether a person could throw a weapon/shield through the detector in an attempt to avoid detection. Additional tests could be conducted to determine how large a quantity could be diverted using this method. Other

tests might be considered that are designed to indicate whether the SPO notes any unusual behavior (for example, the throwing of items through the detector).

- If an individual detector can be defeated, that same detector should be tested again to determine whether such defeat can be repeated. Several tests of the same detector may be required to determine whether a deficiency or given means of defeat can be reliably exploited by an adversary.
- If an individual metal detector can be defeated by one or more methods (for example, walk-through, pass around), the similar metal detectors at other portals should be tested by the same method of defeat in order to determine the extent of the problem. If possible, inspectors should conduct several (three to five) more tests at different portals. If most of these tests indicate the detector can be reliably defeated, there is sufficient evidence to indicate that a systemic problem exists. If no other detectors are defeated, then one may conclude that an isolated deficiency was identified. If the results are inconclusive, the inspector should consider testing additional detectors. Rarely would an inspector test more than five detectors by the same method.

Checklist
Metal Detector
Walk-Through

Interview Items

Installation location _____

Operational test frequency _____

Operational test method _____

Sensitivity test frequency _____

Sensitivity test method _____

False alarm history/records _____

Make/model _____

Tamper protection _____

Provisions for personnel with medical/dental implants that cause alarms _____

Provisions for searching SPOs _____

Tour/Visual Inspection Items

Control settings protected? _____

Occupancy sensor? _____

SPO monitoring method (CCTV, direct)? _____

One-way or two-way traffic? _____

Metal detector used to detect shielding? _____

Package search method? _____

**Data Collection Sheet
Metal Detector – Walk-Through Monitors**

Test Method

	Zone Tested	Portal Location	Operability	Sensitivity	Occupancy Sensor	Detection Capability	Kick	Other
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
<p>Comments:</p>								

Metal Detector—Handheld

Typical Uses

- To detect SNM/shielding on personnel at MAA or PA personnel ingress points (in conjunction with SNM detectors)
- To detect metallic weapons on personnel at PA personnel ingress points
- To investigate anomalies at portals where walk-through detectors are normally used
- To serve as backups if walk-through detectors should fail
- To search at vault exits
- To search at non-routine doors
- To search packages and hand-carried items.

Concerns

- Handheld detectors can be brought very close to areas where metal could be concealed and thus have the potential for detecting very small quantities of metal. However, the effectiveness of the searches is highly dependent on the diligence of the SPOs who conduct them. If the SPO does not search personnel thoroughly (back and front, both sides) or does not take sufficient time, the detection probability can be reduced significantly.
- At portals where traffic is high or when several persons exit in rapid succession, SPOs may be rushed or have difficulty controlling (separating) personnel.
- Proper operation of the detectors by the SPOs is essential for an effective search. Training is also essential to ensure that SPOs can operate the equipment. SPOs should know how to properly position the detector for the most effective searches. Sufficient space that is free of metal, such as rebar in floors or walls, is necessary to properly use the detector and to ensure continuity of operations.
- Handheld detectors may be susceptible to tampering if not adequately controlled.
- Handheld detectors operate on batteries and require regular maintenance.

Types of Tests

- Operability Tests

These tests are conducted to verify proper operability of the detector. They generally involve placing metal near the detector, listening to the detector signal, and verifying an alarm condition.

- Sensitivity Adjustment Tests

Sensitivity adjustment tests are conducted to verify proper detection capability and the SPO's or technician's ability to adjust the detector's sensitivity. Such tests generally involve observing an SPO or technician during performance of routine adjustments. These generally entail placing a specific metal object at a specified distance, listening to the detector signal, and verifying an alarm condition.

- Shielding or Other SNM Capability Tests

Other tests involving shielding material or weapons concealed in a package or on personnel can be conducted as described in this performance test.

Test Guidelines

- Typically, the inspectors conduct operability tests and sensitivity tests at a few key portals (typically two or three).
- If any deficiencies are noted in detector operation or in implementation of search procedures, the inspectors should conduct testing to exploit those deficiencies in order to determine their significance/extent. For example, if the inspectors note the SPOs do not usually search the backside of personnel, the inspectors could design testing to determine whether a person carrying a weapon in his back pocket could exploit the situation and avoid detection.
- If an individual detector can be defeated or does not have proper sensitivity, that same detector should be tested again to determine if such defeat can be repeated. Several tests of the same detector may be required to determine whether a deficiency or given means of defeat can be reliably exploited by an adversary.
- If an individual metal detector can be defeated or does not have proper sensitivity, the similar metal detectors at other portals should be tested by the same method of defeat in order to determine the extent of the problem. If possible, the inspectors should conduct several (three to five) more tests at different portals. If most of these tests indicate the detector can be reliably defeated, there is sufficient evidence a systemic problem exists. If no other detectors are defeated, one may conclude an isolated deficiency was identified. If the results are inconclusive, the inspector should consider testing additional detectors. Rarely would an inspector test more than five detectors by the same method.

Checklist
Metal Detector
Handheld

Interview Items

Location of use _____

How used (backup, normal search, anomaly investigation) _____

Operational test frequency _____

Operational test method _____

Sensitivity test frequency _____

Sensitivity test method _____

Make/model _____

Storage when not in use _____

Tour/Visual Inspection Items

Storage location? _____

Used according to procedure? _____

How traffic controlled? _____

**Data Collection Sheet
Metal Detector – Handheld**

Test Method

	Zone Tested	Portal Location	Operability	Sensitivity Adjustment	Shielding	Other
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
Comments:						

Part 4

X-Ray Equipment Package Searches

Objective	B-67
System Tested	B-67
Scenario	B-68
Evaluation	B-69
Assessing X-Ray Machine Performance	B-69
Interpreting Results	B-69
Special Considerations	B-70
Responsibilities	B-70
Internal Coordination	B-70
Security Considerations	B-70
Personnel Assignments	B-70
Logistical Requirements	B-71
Data Collection Sheet—X-Ray Equipment	B-72

Part 4

X-Ray Equipment Package Searches

Objective

The objective is to test the effectiveness of x-ray machines as tools for searching packages or hand-carried items. The tests discussed here focus on equipment performance. However, the effectiveness of an x-ray search depends heavily on the training and attentiveness of the SPOs who operate the equipment. Other tests may be designed to focus on the effectiveness of procedural implementation, the attentiveness and training of the SPO, or combinations thereof. Such tests require detailed safety plans and are discussed elsewhere.

As per DOE orders, all hand-carried items entering a PA must be searched to prevent the introduction of weapons or contraband. However, the use of x-ray machines is not a requirement for searching hand-carried items; some facilities elect to visually search hand-carried items. X-ray machines are most commonly used at PA entrances. They are used at a few facilities for PA exit (primarily to detect shielding) or at LA entrances to detect contraband. The applicable DOE references are:

Applicability**Order Reference**

Category I and II SNM, Vital Equipment,
PA Entrance

DOE Manual 5632.1C-1,
Chapter V, Paragraph 5

Category I and II SNM, PA Exits

DOE Manual 5632.1C-1,
Chapter V, Paragraph 5

Category I and II SNM, MAAs

DOE Manual 5632.1C-1,
Chapter V, Paragraph 7

LAs

DOE Manual 474.1-1,
Chapter III, Paragraph 5d

System Tested

System - Access control

Functional Element - Hand-carried item entry or exit search

Component - X-ray machine

Scenario

Inspectors should select one or more x-ray machines for testing. The selection is based on a number of factors, including portal configuration and location, operating history, the number of portals, the different types or models of x-ray machines in use, and the types of locations where x-ray machines are employed (for example, PAs, MAAs, LAs).

The inspectors should observe the facility's security alarm technicians or SPOs as they conduct the routine operational or sensitivity tests of selected x-ray machines. During this portion of the test, the inspectors should observe the procedures to determine whether the tests, calibrations, and maintenance measures are consistent with DOE orders and approved SSSPs, and whether they are an effective means of testing the systems. The inspectors accomplish two goals by having the facility's security technicians conduct the routine tests before testing by inspectors. First, the facility's tests indicate the effectiveness of the test and maintenance program. Second, the facility's tests should verify that the detectors are calibrated according to facility specifications; thus, the inspectors are assured that the system is operating as the facility intends. This may be important in identifying the root cause of deficiencies.

Inspectors should conduct sensitivity tests using stepwedges or wire gauge standards. The purpose of these tests is to determine whether the x-ray machines are properly calibrated and have sufficient penetrating power. These tests simply involve passing a stepwedge through the x-ray machine and determining resolution and penetration capabilities.

The inspectors may also place objects in a briefcase (which may be aluminum, leather, or other material) and observe resolution capability. Resolution capability tested by this method is somewhat subjective. One useful test procedure is to oversee an SPO who is monitoring an x-ray machine: What types of objects alert the SPO to visually examine the items? Also, the inspectors can place an object that is opaque (such as a steel box) in a briefcase and pass it through the x-ray machine to determine whether the SPO directs the briefcase to be opened and the contents examined to verify that contraband is not concealed.

The number of x-ray machines selected for testing depends on the time available, the importance of the system in the overall protection program, and the variation in the types of x-ray machines used at different portals. The following guidelines are intended to assist the inspector in selecting detectors for testing:

- At very small facilities, or at facilities with only a few (that is, less than five) x-ray machines, the inspectors may elect to test all units. At larger facilities, the inspectors would typically select x-ray machines at two to four portals for testing.
- Entry searches at PA portals are required by DOE orders. Some facilities conduct searches at MAA exits in addition to the PA entry searches. A few facilities conduct entry searches at MAA entrances instead of at PA entrances; this procedure requires an approved exception to DOE orders. The inspectors should determine where entry searches are conducted and focus their efforts on the locations that are more critical from a security perspective.
- If the first few tests reveal no problems and there is no evidence of exploitable deficiencies, the inspectors should not generally devote extensive time to testing numerous additional x-ray machines. However, if deficiencies are apparent, the inspectors should collect sufficient data (by testing additional x-ray machines) to determine whether a deficiency is an isolated instance or a systemic problem.

Evaluation

For the searches to be effective, the x-ray machine must be part of an integrated system consisting of hardware, personnel, and procedures. This section deals primarily with the evaluation of the x-ray machine hardware. Guidance is provided on assessing effectiveness and interpreting results.

Assessing X-Ray Machine Performance

The primary objective in evaluating an x-ray machine is to determine whether that machine is capable of imaging a 24-gauge wire and has sufficient penetrating power to clearly display objects contained in a briefcase. Other points that should be considered in the evaluation are:

- Are there provisions for monitoring personnel possessing hand-carried items to ensure that normal procedures are followed? For example, are there provisions for ensuring that personnel do not bypass the search?
- Is the system of barriers and procedures at the portal sufficient to ensure that hand-carried items are not passed around the search location?
- Are the SPOs who operate the x-ray machines trained in the use of the equipment, and are they familiar with the search procedures?
- Are response procedures clear, complete, and sufficient to ensure that all anomalies are resolved before allowing ingress or egress?
- Can SPOs prevent toss-through?
- Are provisions adequate to ensure that unauthorized personnel do not tamper with the x-ray machines and do not have access to control settings?
- Are testing and maintenance procedures sufficient to ensure that the x-ray machines are reliable and correctly calibrated?
- Are personnel safety procedures documented and available as per 21 CFR 1020.40(c)?

Interpreting Results

The following guidelines are provided to assist the inspectors in interpreting results in the context of system performance:

- Tests that indicate the x-ray machines can be bypassed or do not have sufficient resolution capability or penetrating power are evidence of a potentially serious deficiency. The significance of such deficiencies must be analyzed in the context of site-specific protection objectives and the effectiveness of other complementary systems. Deficiencies in x-ray machines used for entry searches lead to the potential for adversaries to introduce weapons into a security area. Additional layers of searches (for example, at both the MAA and PA) may partially mitigate deficiencies in x-ray machines.
- Slightly improper calibration or lack of sensitivity is significant, but much less serious than gross errors in calibrations or exploitable deficiencies. Such results would indicate improper calibration or

slight lack of resolution capability, but not necessarily a serious vulnerability. These results could indicate a potential testing and maintenance deficiency, and the inspectors should consider conducting additional tests to determine whether the improper calibration is an isolated case or a systemic problem.

Special Considerations

Inspectors may have access to wire standards and stepwedges that may be used for performance tests. Alternatively, they may use wire standards, stepwedges, or similar items provided by the facility. The inspectors should contact the facility early in the planning process to determine what types of test items are readily available.

Related testing and activities, such as SNM detector tests and reviews of portal barriers and procedures, are typically conducted concurrently with x-ray machines tests to increase the efficiency of data gathering.

Responsibilities

Inspectors: Select the portals and x-ray machines. Direct testing and observe resolution capability and penetration power.

Facility: Conduct routine testing. Assign SPOs to provide security during testing, as required. Provide security technicians to conduct testing at the direction of the inspectors.

Internal Coordination

Testing should be scheduled to avoid conflicts with other tests involving the protective force.

Security Considerations

All normal security considerations should be observed. Normally, a protective force representative must monitor tests to ensure that security is maintained.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Alarm technicians

Equipment

- Wire standard
- Stepwedge
- Briefcase (aluminum)
- Briefcase (leather, vinyl, or other non-metal material)

Safety

- Follow normal operating procedures
- Complete a safety plan
- Notify the CAS and other alarm monitoring stations before any tests are conducted
- Continue to prevent any undesirable armed response by the protective force to alarms

**Data Collection Sheet
X-Ray Equipment**

Test Method

	Zone Tested	Portal Location	Operability	Sensitivity	Other
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					