

APPENDIX E

PERSONNEL AND PROCEDURE PERFORMANCE TESTS

Part 1: General Background	E-1
Part 2: Candidate Procedures.....	E-5
Part 3: Sample Scenarios.....	E-11
Part 4: Badge Checks	E-15

Part 1
General Background

Introduction	E-1
Test Design, Conduct, and Evaluation	E-2
Scenario	E-2
Evaluation Criteria	E-3
Responsibilities	E-3
Logistics	E-3
Safety Concerns	E-3
Performance Test Plan	E-4
Coordination	E-4
Scheduling	E-4
Conduct	E-4
Evaluation	E-4

Part 1

General Background

Introduction

In addition to tests of physical security equipment, the inspectors may elect to design and conduct performance tests that stress the facility's security-related procedures and the personnel who perform security-related tasks.

Personnel and procedures are an essential part of an effective security program at all DOE facilities. Many DOE facilities do not have sophisticated automated security hardware and rely heavily on personnel and procedures to perform security functions such as searches and intrusion detection. Procedural controls are necessary for many aspects of security including material transfers, material surveillance, patrols, alarm response, entry control, badge issuance, and visitor control. Trained, dedicated, and alert personnel are necessary to implement procedures and interface with security equipment. At a typical facility, security-related procedures are implemented by a wide range of personnel and facility organizations, including members of safeguards and security, testing and maintenance, operations and production, personnel security, and management.

Although personnel and procedures are an essential part of a PSS, it is frequently more difficult to test the effectiveness of personnel and procedures during an inspection than it is to test equipment. When designing, conducting, and evaluating tests of personnel and procedures the inspectors must consider the following complexities:

- Procedures are site-specific.
- Procedures are not always formally documented.
- Procedures are not always current.
- “Real world” implementation may vary from documented procedures.
- Effectiveness varies from person to person.
- Individual motivation and alertness levels vary.
- An atmosphere of heightened security awareness exists during an inspection.
- Safety must not be compromised.
- The element of surprise may be difficult to simulate.
- Tests are not always repeatable (e.g., an SPO may find a contraband item in a briefcase one time but not the next).

Because of these complexities, testing of personnel and procedures requires extensive planning. However, in many cases, these tests provide valuable information on the effectiveness of the overall system. The inspectors must examine their resources and information needs and determine whether the benefits of the

information gained from personnel and procedures testing is worth the resource expenditure necessary to design and conduct them, or whether resources are better spent on other activities.

Test Design, Conduct, and Evaluation

As part of the normal inspection activities, the inspectors should review the security systems, including equipment and procedures. When the inspectors identify a procedure critical to system effectiveness, they should consider designing a performance test to provide information on the effectiveness of that procedure.

Part 2 of this appendix provides a “laundry list” of typical procedures or personnel actions that are candidates for testing. Other candidate procedures may be identified by the inspectors. Once the inspectors decide to conduct a test, they would generally follow the steps listed below:

- Develop a scenario.
- Determine evaluation criteria.
- Assign responsibilities.
- Arrange logistics.
- Address safety concerns.
- Develop a performance test plan.
- Coordinate with other topic teams.
- Schedule testing.
- Conduct testing.
- Evaluate results.

Scenario

A scenario is a detailed description of the activities inspectors will conduct (or direct the facility to conduct). The scenario activities are designed to provide an opportunity for the inspectors to observe the system response under controlled conditions. This may involve setting up a situation in which the inspectors can observe whether personnel follow procedures and whether an objective of a procedure is achieved (for example, detect a weapon in a visual search of a briefcase). Sample scenarios are included in Part 3 of this appendix. The scenarios in Part 3 are not intended to be a comprehensive set but rather are intended to guide the inspectors in their development of site-specific scenarios.

Development of scenarios usually requires the involvement of a facility representative to act as a trusted agent. The trusted agent helps the inspectors design the tests and arrange logistics while maintaining confidentiality so the test is not compromised.

Where necessary, the scenario should include provisions for repeating a test with different persons or at a different location in order to provide sufficient data to draw valid conclusions. For example, a test

involving a weapon in a briefcase might be conducted at three different locations. If one SPO fails to conduct a thorough search and misses the item, the facility may argue that it was a random occurrence. However, if three SPOs do not conduct thorough searches, then the inspectors may conclude that procedures are not diligently implemented and a systemic problem exists.

Evaluation Criteria

The inspectors should thoroughly understand what to expect during a test and what the site-specific objectives are for the tested element. The inspector should document the evaluation criteria in the performance test plan. The evaluation criteria must be consistent with DOE orders.

Responsibilities

The responsibilities for conducting these tests should be clearly defined. This includes identifying the field element's responsibilities as well as those of each inspector.

Logistics

The inspectors should carefully coordinate all logistical aspects of the tests. Items to be considered include:

- The need for equipment, test sources, and standards.
- The need for special personnel, such as health physics technicians, to conduct various steps of the test.
- Any requirements related to operating conditions (for example, day or night, access or secure mode).
- The need for additional security measures.

If observers (other than the persons involved in the test) are necessary, arrangements should be made to station them where they will not interfere with the test or confuse or otherwise influence the personnel being tested.

Safety Concerns

Testing should be conducted with the highest regard for safety. The inspectors should be certain that adequate measures are implemented for ensuring that:

- Armed response is prevented or controlled.
- Exposure to radioactive or toxic material is avoided or minimized.
- Facility, DOE, and other safety procedures are strictly followed.
- The inspectors and facility have adequate means to interrupt or cancel the test if safety is compromised or if an actual safety or security situation arises during the test.

Performance Test Plan

Performance test plans should be developed and included in the inspection guides. The performance test plan should be sufficiently detailed so that a reviewer would understand the basic scenario and evaluation criteria. Safety measures should also be included. Responsibilities should be defined. A sample performance test plan, used for testing the effectiveness of badge checks, is included as Part 4 of this appendix.

Coordination

The inspectors should coordinate with other topic teams before conducting testing in order to avoid overlapping or conflicting activities. Other teams may be interested in the test results and may assist with the testing or send observers. The teams should ensure that tests that may conflict with each other are not scheduled simultaneously. For example, testing the response to an intrusion alarm may result in facility lockdown, which could interfere with other tests.

Scheduling

Testing should be scheduled in advance, allowing time for management review, coordination, and safety reviews. Information related to tests that rely on “surprise” (for example, tests for contraband in a briefcase or an alarm response test) should be carefully controlled to decrease the likelihood of compromising the test.

Some tests need to be conducted under certain operational conditions (for example, night shift). These tests should be conducted as realistically as possible.

Some tests may have to be repeated several times or in more than one location to provide sufficient data for evaluation purposes. Such testing should be scheduled accordingly, with consideration given to the likelihood that the “word” will spread quickly when a test is conducted, and subsequent results may be biased.

Conduct

The test should be conducted according to the test plan, with as little deviation as possible. If any deviation is necessary, the inspectors, in conjunction with the facility representatives, should verify that safety is not compromised and that the objectives of the test are still valid. The inspectors should be prepared to interrupt or cancel the test whenever a safety concern is identified and should have a means of promptly notifying all personnel when such an action is deemed necessary.

Evaluation

Performance test results are evaluated against DOE orders and site-specific objectives. Performance tests are not individually rated. Instead, the information gathered in the test is factored in with other information collected during interviews, other tests, and document reviews, and the overall effectiveness of the system is evaluated.

Part 2

Candidate Procedures

Introduction	E-5
Entry Control Systems	E-5
Barriers	E-6
Intrusion-Detection Systems	E-7
Testing and Maintenance	E-8
Auxiliaries and Interfaces	E-9

Part 2

Candidate Procedures

Introduction

This section lists the procedures and personnel actions that are candidates for performance testing by the physical security systems inspection team. The inspectors may identify other procedures that are suitable for testing during the site-specific reviews.

Entry Control Systems

General

- Procedures to verify access authorization by checking identifiers (for example, names, employee numbers) against an access authorization list (hard copy or computer file)
- Procedures to log non-routine entries (for example, visitors, personnel during off-shift, and personnel not normally assigned) at security areas
- Procedures to verify the identity of a visitor before issuing a badge/pass/credential
- Procedures to verify the authorization and clearance of a visitor before issuing a badge/pass/credential
- Procedures to verify the access authorization of vehicles

Badge Systems

- Badge checks by SPOs at MAAs, PAs, LAs, or other security areas
- Procedures to store and account for badges
- Procedures to report lost badges and notify appropriate personnel
- Badge/personnel identification checks at portals that use CCTV to verify identity of personnel entering a security area

Automated Systems

- Procedures to store and account for coded credential devices (for example, cards, and stocks of blanks)
- Procedures to enroll personnel in an automated access control system (for example, card reader, biometric identification device)
- Procedures to delete personnel from an automated access control system

- Procedures to monitor personnel as they interface with access control equipment to ensure they follow authorized procedures

Searches

- Use of handheld equipment (for example, metal detectors) to search personnel entering a security area
- Use of handheld equipment (for example, metal or SNM detectors) to search personnel leaving a security area
- Procedures to monitor personnel passing through walk-through SNM or metal detectors
- Use of handheld equipment (for example, SNM detectors, mirrors) and visual inspection techniques to search vehicles entering or leaving a security area
- Procedures to search hand-carried items or packages entering or leaving a security area (including visual, x-ray, or SNM detector searches)
- Procedures to search packages too large to pass through an x-ray machine
- Procedures to search packages unsuitable for visual inspection (for example, sealed components)

Barriers

General

- Procedures to patrol and inspect exterior security area perimeter barriers (for example, fences) to verify integrity and detect unauthorized objects (for example, ladders) or conditions (for example, excessive soil erosion under fence)
- Procedures to patrol and inspect interior security area perimeters barriers (for example, MAA walls, doors, windows) to verify integrity and detect penetration
- Procedures to patrol and inspect security containers to verify they are locked/secured
- Procedures to patrol and inspect vehicle barriers to verify integrity
- Procedures to inspect activated barriers to verify integrity and detect tampering
- Procedures to lock down a facility or area in response to a security condition

Lock and Key Controls

- Procedures to issue keys
- Procedures to store keys

- Procedures to change locks and lock cores
- Procedures to issue combinations
- Procedures to change combinations

Intrusion-Detection Systems

Electronic Intrusion Alarm Systems

- Procedures to assess intrusion alarms
- Procedures to assess tamper and line-supervision alarms
- Procedures to respond to alarms, including response time; also, response procedures when multiple alarms occur simultaneously
- Procedures to record/log alarms
- Procedures to patrol perimeters and security areas and to inspect systems to ensure that protection is not degraded (for example, verify that no ladders, scaffolds, or equipment that could be used to bridge/jump the exterior sensors are in isolation zones, verify no equipment blocking interior sensors)
- Compensatory procedures used during failure of alarm system or components thereof
- Procedures to place alarms in access mode and return them to service mode

Lighting

- Procedures to patrol or inspect areas and identify/correct lighting deficiencies, including burned-out bulbs
- Compensatory measures used during failure of lighting systems

Visual Detection

- Procedures to continuously monitor perimeters or areas
- Procedures to patrol perimeters or areas

CCTV Assessment Systems

- Procedures to assess alarms
- Procedures to track intruders using CCTV with PTZ features
- Procedures to periodically verify operability of CCTV systems that are not continuously displayed (for example, call-up or sequenced monitors)

Communications Equipment

- Procedures used to communicate a duress situation when duress switch cannot be activated, such as use of code words
- Procedures to respond to a duress condition

Radio Systems

- Investigation/response procedures implemented if an SPO does not respond to a periodic radio check
- Procedures to switch to different frequencies during specified conditions (for example, tactical response)

Other

- Procedures to use other systems as a backup if primary system capability is lost
- Procedures to use PA systems to direct plant personnel during security situations or emergency evacuation conditions

Testing and Maintenance**Testing**

- Procedures to test security-related hardware
- Procedures to report incorrectly calibrated or inoperable equipment
- Procedures to record test results

Calibration/Preventive Maintenance

- Procedures to maintain/calibrate security-related hardware
- Procedures to initiate repair/replacement of degraded equipment
- Procedures to record maintenance results

Corrective Maintenance/Repair

- Procedures to isolate/locate causes of failures
- Procedures to repair/replace components
- Procedures to record repair/maintenance

Quality Assurance

- Procedures to verify test results
- Procedures to verify proper maintenance (for example, functional tests by second person)
- Procedures to verify work by vendors
- Procedures to inspect new components and components repaired by offsite vendors
- Procedures to verify integrity of system following software modification

Auxiliaries and Interfaces

Protective Force Procedures

- Procedures to respond to evacuations caused by fire, criticality, or other emergency situations
- Procedures to escort SNM shipments
- Procedures to verify SNM transfer authorization
- Special post orders
- Procedures to patrol areas

Production/Operations/Health Physics/Safeguards Department Procedures

- Procedures to maintain material surveillance
- Procedures to verify SNM transfer authorization
- Procedures to transfer SNM
- Procedures to verify non-SNM transfers out of an MAA
- Procedures to control SNM during/following an emergency evacuation and safety situation (fire, accident)
- Procedures to enter/secure a storage area

This page is intentionally left blank.

Part 3

Sample Scenarios

Introduction	E-11
Scenario 1—Badge Checks	E-11
Scenario 2—Perimeter Patrols	E-11
Scenario 3—Maintenance Personnel	E-12
Scenario 4—Visual Detection	E-12
Scenario 5—Emergency Evacuation	E-12

Part 3

Sample Scenarios

Introduction

This section presents five sample scenarios for performance tests of personnel and procedures. These samples represent a wide range of test-design complexity. Inspectors will also likely develop scenarios for testing other procedures. Any scenarios developed to test a site-specific procedure that are proven effective and are applicable to other facilities should be submitted to OA-10 for incorporation into the appropriate inspectors guide.

Scenario 1—Badge Checks

At facilities that rely on badge checks to control entry into a security area, the inspectors may test the effectiveness of the badge checks (in particular the alertness of the SPO) by using the following scenario:

- Arrange for a person who normally accesses a security area to attempt to gain access to that area by using a badge that has incorrect or outdated information.
- Arrange with Badge Office to obtain an “improper” badge—that is, a badge that does not meet the facility’s requirements. The improper badge may be expired (if dates are included on badge), may have the right name but wrong person’s picture (or vice versa), or may omit an authorization symbol specific to that area. Alternatively, the person may attempt to enter using a different person’s badge.
- Have the person follow normal procedures to enter the security area, preferably during high-traffic periods or when the SPO is likely to be rushed.
- Determine whether the SPO checks the badge as per procedures, detects the improper badge, denies entry to the person, and responds to the unauthorized attempt as per procedures.

Scenario 2—Perimeter Patrols

Facilities that have perimeter alarm systems must periodically patrol the alarmed perimeter to reduce the risk of adversaries defeating alarm systems through bridging techniques. The following scenario is one method of testing the effectiveness of patrols, in particular the alertness and training of the SPO on patrol. This scenario is particularly applicable at facilities that do not frequently monitor the perimeter with CCTV, that have relatively small isolation zones (for example, 12 feet or less from fence to fence), and that do not use fence-mounted sensors. Inspectors should:

- Arrange for the facility to provide an extension ladder
- Direct a facility representative to covertly place the extension ladder near the fence line or, if feasible, across the tops of the two fences, such that an adversary could use the ladder to crawl across the isolation zone without entering the sensor detection zone. The ladder should be placed in a location that is not visible from a protective force post, preferably after dark.

- Monitor CAS operations and radio systems to determine when (or if) the protective force patrol identifies a potential security concern, whether program reporting procedures were followed, and whether appropriate response was initiated.

Scenario 3—Maintenance Personnel

The effectiveness and knowledge of maintenance personnel can be tested by the following scenario:

- Arrange with the facility to intentionally disable a security component shortly before a routine calibration. For example, a lead on one channel of an SNM walk-through monitor could be disconnected.
- Observe maintenance team members during their routine calibration procedure and determine whether they correctly identify the problem and initiate corrective action.

Scenario 4—Visual Detection

Facilities that rely on visual detection at a security area can be tested with the following scenario:

- Arrange for a small team (one or two) of facility representatives or inspectors to dress in dark clothing.
- Plan an entry route to the facility that avoids “heavy population” areas and well-lighted areas, maximizes the use of cover and concealment, and avoids the direct view from SPO visual observation posts.
- Have the “adversary” attempt to enter the facility along the planned route.
- Determine whether the SPOs in observation posts or on patrol detect the “adversary” before gaining access to a security area.

Scenario 5—Emergency Evacuation

Facilities that have SNM must protect it during an emergency evacuation. The following scenario may be used to observe the protective force response to a simulated evacuation when the protective force procedures call for an SNM “sweep” of the area following the evacuation. Inspectors should:

- Choose a convenient time, preferably causing minimal impact on operations, and when no SNM is out of secured storage (to ensure that security is not degraded by the test).
- Station an “adversary” possessing a radioactive source (non-SNM) near an MAA emergency exit.
- Direct a facility representative to simulate a criticality alarm and direct personnel to evacuate (the personnel should be informed that it is a test and to exit at controlled speed to minimize safety concerns).
- Direct the “adversary” to exit the area as soon as the “criticality alarm” is sounded and, drop the radioactive source in a location suitable for later pickup (for example, a trash can) before proceeding to his/her designated assembly point.

- Observe the protective force's response to the evacuation alarm and its procedures for controlling exiting personnel.
- Determine whether the protective force locates the radioactive source during the SNM sweep.

This page is intentionally left blank.

Part 4

Badge Checks

Objective	E-15
System Tested	E-15
Scenario	E-15
Evaluation	E-16
Special Considerations	E-17
Responsibilities	E-18
Internal Coordination	E-18
Security Considerations	E-18
Logistical Requirements	E-18
Safety	E-19
Personnel Assignments	E-19

Part 4

Badge Checks

Objective

The objective is to test the effectiveness of the badge checks in detecting and preventing unauthorized entry attempts. Specific tests may focus on the effectiveness of procedural implementation, the tamper-resistance of the badge, the attentiveness and training of the SPOs, or combinations thereof. The applicable DOE references are:

Applicability	Order Reference
Category I and II SNM, PA	DOE Manual 5632.1C-1
Category I SNM, MAA	DOE Manual 5632.1C-1
Vital Equipment, Vital Area	DOE Manual 5632.1C-1
Category III SNM	DOE Manual 5632.1C-1
Category IV SNM	DOE Manual 5632.1C-1
Classified Matter, Limited Area	DOE Manual 5632.1C-1
Government Property and Unclassified Facilities	DOE Manual 5632.1C-1

System Tested

System	- Access control
Functional Element	- Personnel identification and verification
Component	- Badge check at security area portal or security checkpoint.

Scenario

Option 1—Authorized Person/Incorrect Badge

The inspectors should arrange for a person who normally accesses a security area to attempt to gain access to that area by using a badge that has incorrect or outdated information.

- Arrange with the badge office to obtain an “improper” badge. That is, a badge that does not meet the facility’s requirements. The improper badge may be expired (if dates are included on badge), may have the right name but wrong person’s picture (or vice versa), or may omit an authorization symbol specific to that area. Alternatively, the person may attempt to enter using a different person’s badge.
- Have the person follow normal procedures to enter the security area, preferably during high-traffic periods or when the SPO is likely to be rushed.
- Determine whether the SPO checks the badge as per his procedures, detects the improper badge, denies entry to the person, and responds to the unauthorized attempt as per procedures.

Option 2—Unauthorized Person/Fake Badge

The inspectors should arrange for a person who is not authorized access to a security area to attempt to gain access to that area using a fake badge.

- Obtain a badge for an unauthorized person. The easiest way of doing so is to use the badge of an authorized person, preferably one who bears some physical resemblance to the person attempting entry. Alternatively, arrange with the badge office to obtain a badge, insert, or stock for the person(s) attempting entry. Depending on the specifics of the facility’s operations and the test objectives, the badge may be correct in every detail or may be flawed in one or more aspects (for example, improper lamination to simulate an adversary who has tampered with the badge).
- Have the person follow normal procedures to enter the security area, preferably during high-traffic periods or when the SPO is likely to be rushed.
- Determine whether the SPO checks the badge as per procedures, detects the improper badge, denies entry to the person, and responds to the unauthorized attempt as per procedures.

Evaluation

The primary factor in the evaluation is whether the objectives of the badge check were met, that is, whether the unauthorized access attempt was detected and entry denied. Other questions that should be considered in the evaluation are:

- Did the SPO correctly follow all procedures when checking the badge?
 - If holding or touching the badge is required, did the SPO do so?
 - If the badge is in a clear plastic holder and touching the badge is part of the procedure, did the SPO remove the badge from the holder?
 - If access codes are included on the badge, were they checked before entry was allowed?
 - If a badge exchange is part of the procedure, was it performed correctly?
 - Did the SPO assure that the person attempting entry removed sunglasses or other articles in order to facilitate comparison?

- Did the SPO correctly identify discrepancies with the badge (if any), such as:
 - Wrong person’s picture?
 - Wrong name?
 - Expired?
 - Wrong access code?
- If checking the name or badge number against an access list is part of the procedure, did the SPO correctly do so?
- Were applicable entry logs (if any) filled out correctly?
- If a discrepancy is detected, did the SPO deny entry and follow the appropriate response procedures such as:
 - Detain suspect?
 - Call supervisor and backup?
 - Shut down portal (if required)?
 - Other?

The specific objectives of the test should be kept in mind during the evaluation. Tests involving a normally authorized person with an incorrect badge are primarily designed to determine how attentive the SPO is and how thoroughly the badges are checked. Tests involving an unauthorized person are primarily designed to determine whether an adversary can use a fake badge to gain entry. Other factors to consider when evaluating the test results include:

- Are there any related or complementary systems that perform the personnel identification function, for example, a card reader in conjunction with the badge check or a requirement for an escort with every visitor?
- Is there more than one layer in the system that an adversary would have to pass to gain access to security interests?
- Are controls inside the security area likely to be effective or is the adversary essentially unrestricted once inside the area?

Special Considerations

More than one badge test should be conducted in order to gain a more complete assessment of effectiveness. If possible, at least three, and preferably more, such tests should be conducted. However, the inspector must recognize that once the first test is complete, the “word” will spread quickly and the protective force will be more alert. If possible, several locations should be tested in a short time interval; for example, essentially simultaneous tests conducted at three different MAAs. Tests during high-traffic periods (for example, shift change) are desirable.

The locations selected for badge tests should be based on consideration of all pertinent factors, including:

- The potential impact of an unauthorized entry to the area
- Other complementary systems
- The number of layers in the system: LA, PA, MAA
- The number of personnel assigned to the area and the procedures for SPO rotation (personnel recognition)
- Throughput rates at portals.

Badge tests should be conducted as unobtrusively as possible in order to realistically simulate normal conditions. A crowd of observers will likely influence the actions of the SPO. If possible, the inspector should arrange to discreetly observe the test (for example, by CCTV at the CAS).

Responsibilities

Inspectors: Select the type of fake badges needed and request the facility to provide them without alerting SPOs. Select the portal(s) that will be tested and the time(s) of the tests. Select and provide instructions to the adversaries.

Facility: Provide fake badges as needed. Provide assistance in finding adversaries. Address safety concerns and assure that protective force supervision is available to control response.

Internal Coordination

Test results are also of interest to the protective force topic team as they relate to training and duties. Tests should not be scheduled such that they would interfere with other tests involving the protective force.

Security Considerations

All normal security procedures should be followed. If an unauthorized person successfully gains access to a security area, measures should be taken to assure that he is not permitted access to classified matter.

Logistical Requirements

- Fake badges may be needed from the badge office.
- A protective force supervisor should be available to control activities at each portal where a test is conducted.
- Observers, if any, should be kept from influencing the test results. Observation by CCTV at a remote location is desirable.

Safety

- Normal operating procedures should be followed.
- Protective force supervisors should assure that the SPO's response can be controlled.
- A safety plan should be completed.

Personnel Assignments

Test Director:

Facility Trusted Agent:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

This page is intentionally left blank.