DEVELOPING AND CONDUCTING PERFORMANCE TESTS

The following guidance relating to the development and conduct of performance tests was pulled from the Office of Independent Oversight, *Protective Force Inspectors Guide*, October 2009. For a complete version of this document please contact the Office of Health, Safety and Security Office of Enforcement and Oversight.

Determining Test Objectives

Before serious planning can commence, the objective(s) of the test must be clearly defined and stated. This is necessary whether or not the type of test can meet more than one objective. For example, an Entry Control Performance Test could test the adequacy of entry control procedures, or it could test a Security Police Officer's ability to properly apply those procedures. Detailed planning must be aimed at satisfying clearly understood objectives. The objective may be to see whether all protective force flashlights work, or whether all rifles are properly battle-sight zeroed, or whether protective personnel can properly perform certain specific skills or adequately execute specific procedures.

Determining Test Attributes

After determining the test objectives, the planner must select a testing protocol that provides maximum achievable realism, assures adequate safety, and satisfies the test objectives. This determination involves several components:

- How to Test - The type of performance test and specific testing techniques must be determined. Test objective, realism, safety, available resources, and all other applicable variables must be considered in determining an acceptable testing method. The planner has to determine what skill, duty, or function is to be tested, and then devise the best method of testing it. The best way to test is to make the subject actually demonstrate the skill, perform the duty, or operate the equipment under conditions that are as realistic as possible.

- Where to Test - Test location is important and, in some cases, has a significant impact on realism. Generally, the best location is the location where the event being tested would actually occur. For example, if the test is to determine the tactical skills of the protective force in protecting the vital areas of a reactor, the test should be conducted at the reactor. An acceptable alternative might be a similar reactor that is off-line or shut down. A poor alternative would be a non-reactor building or facility which does not resemble a reactor. If testing entry control procedures, the tests should be conducted at actual entry portals, preferably at a representative sample of such portals.

- When to Test - The timing of the test also affects realism. When testing night firing skills, it's best to test at night. When testing day shift personnel on felony vehicle stop procedures, it's best to test in daylight. When testing entry control procedures, it's best to conduct the bulk of the tests during normal working hours, including shift change, when most entries and exits occur. When testing an event that would normally take place at a crowded facility, the test should take place when the facility is crowded, not after hours when it is deserted except for protection personnel.

- How Many Tests to Conduct - The number of iterations of a particular performance test will depend on the nature of the test and the available resources. Detailed planning requires an early determination of the number of tests to be conducted; this is especially true of complex tests and tests involving large numbers of personnel or use of scarce facilities.

Scenario Development
Once preliminary decisions such as test objectives, location, and time have been made, planning of specific scenario events can begin. The scenario consists of those events that create the situation that will test the subject. The complexity of the scenario is directly related to the complexity of the test. For example, an LSPT might be conducted to determine whether flashlights work. The scenario would be as simple as to switch on the selected flashlights and see if they illuminate.

Scenario development requires the planner to devise and think through a logical series of events that will elicit realistic responses and accomplish the test objective. As scenarios become more complex, particularly those involving adversaries and tactical procedures, there will be a wide range of scenario event options. It is important to judiciously choose among the options to select events that are realistic, within the appropriate threat guidance, and logical (in the sense of the flow of scenario events), and that also serve to fully satisfy the test objective. It is helpful to keep scenario events as simple and straightforward as possible unless there is a specific requirement to include intricate or complicated events.

For large-scale ESS performance tests, Independent Oversight normally develops the scenarios based on the objectives, which will then be coordinated closely with the site trusted agents to ensure the test objectives can be exercised. The primary trusted agents from both the site and Independent Oversight will give written concurrence agreeing to the scenarios.

Simulation
There is some amount of simulation or artificiality in most performance tests. To preserve realism, it is best to keep simulation at a minimum. Performance tests involving live adversaries usually require the greatest amount of simulation, generally because of safety or test control requirements. The following are some typical simulations encountered in protective force performance tests:

- Response Times - To keep protective force players within the test area, it is frequently necessary to place players who would normally respond from outside the test area into a holding area and release them into test play according to a predetermined schedule. The best way to determine the release schedule is to conduct a no-notice response test and record the actual response time for each responder.

- Explosives - Typically, inert dummy explosives and related equipment are carried, and deployed as actual explosives would be. A controller is required to verify that the explosives are properly set, at which time he/she simulates the effects of the explosives, which may include throwing a grenade simulator, opening a door or gate, and assessing casualties.

- Initial Player Positioning - At times, adversaries are pre-positioned in the test area. For example, in Containment Performance Tests, it is usual to place the adversaries inside the target building before the test. If this approach is taken, the protective force players must be briefed on the simulated events (through alarm chain, eyewitness observations, etc.) by which the adversaries entered the building. Similarly, protective force players are sometimes pre-positioned in their response positions or in a holding area for scheduled release. These positions may have been determined based on previous observations of routine posts and patrol activities.

- Personnel and Time Limits - At most sites, over a period of time, more and more protective personnel and local law enforcement personnel would be able to respond to a security incident. For test purposes it may be desirable to limit protective force players to a manageable yet realistic number; for example, those personnel in a target area and those who could respond to the area

within 15 minutes. Utilizing this strategy, it is reasonable to also limit the running time of the test, so that the protective force players do not have to continue long after they would have realistically received more resources.

- Target Material - If special nuclear material or other sensitive devices are involved in scenario play, it is usually simulated using other materials or devices of similar size, weight, and configuration.

- Location - If the actual facility or building cannot be used, the test must be conducted at an alternative location. The layout and attributes of the test facility should be as similar as possible to the actual facility.

- Controller Presence/Actions - The mere presence of controllers is artificial, but necessary. At times, controllers must simulate scenario events, such as alarms, explosive effects, and breaching of barriers, or they may have to intervene to enforce safety rules or rules of engagement. Generally, controllers should intervene in test play only when necessary and otherwise avoid interfering with test play.

Control Measures

Conducting an orderly and safe test requires the planning and enforcement of various control measures. Some control measures are restrictive, so it is important to strike a balance between the need for realism and the need to control the test. Without being overly burdensome, sufficient control measures should be planned to ensure that the scenario can be executed properly and realistically, the test can be conducted safely, and the necessary degree of control can be exerted by the Exercise Coordinator during the entire test. Control measures generally apply to both sides and the desired condition is that the cumulative effect of all control measures be neutral. The following are some typical control measures:

- Boundaries - Boundaries establish the limits of the test area. Players are not allowed to leave the test area, and armed protective personnel are not allowed to enter the test area except under controlled conditions.

- Off-Limits Areas - At times, certain areas (rooms, buildings, rooftops, and excavations) within the test area boundaries must be placed off limits, usually for safety or operational reasons. Radiation areas, construction areas, and rooms where armed protective personnel are sequestered are typically placed off limits. These areas are off limits to players on both sides and frequently off limits to controllers and other non-player participants also. Locations of off-limits areas must be fully explained, and they must be locked, marked, or otherwise physically identified to all participants. The number of off-limits areas should be kept to a minimum. As agreed to by safety and operational trusted agents, it is sometimes sufficient to caution participants about the hazards in an area rather than place the area off limits.

- Rules of Engagement - This is a set of rules by which players on both sides must abide during tests involving live adversaries. While there is a fairly standard set of rules of engagement, they may be amended as conditions require for each test. For more details on specific rules of engagement, see *Protective Force Protocols and Rules of Engagement*, March 12, 2007.

- Safety Rules - This is a set of safety-related rules by which all test participants must abide. There is a fairly comprehensive set of standard safety rules. These rules are normally modified to accommodate the scope and nature of the specific performance test and site-specific safety requirements.

- Controller Actions - Controllers are responsible for enforcing the rules of engagement, conduct, and the safety. They may also have specific preplanned or spontaneous responsibilities, such as opening doors, passing messages to alarm station operators, releasing responders from a holding area, or assessing casualties.

- Communications - In any test where not all participants are at the same restricted location, reliable communication is essential. The Exercise Coordinator must be able to communicate directly with all evaluators and either directly or indirectly with all controllers and players. Suitable methods of coordinating with the shadow force or summoning an ambulance, if necessary, must be established.

- Test Initiation and Termination - Conditions for starting and stopping the test must be established. Generally, a test is started when all participants are in place and all safety and other requirements are satisfied. Conditions and procedures for temporarily stopping the test must be established and briefed to all participants prior to the start of the exercise. Temporary delays should be avoided if possible, but are occasionally caused by safety or security incidents or administrative holds to reposition players during an FOF. Conditions for terminating the test are usually based on completion of the test scenario or reaching a predetermined time limit, but may also include the occurrence of a major safety or security event at the site, whether or not it involves test participants.

Logistics

Some logistical planning is necessary for even the simplest performance test; complex tests may require extensive and detailed logistical planning. While the trusted agents are responsible for accomplishing most of the logistical tasks, it is up to the Exercise Coordinator to ensure that all logistical needs have been identified and that the trusted agents deliver the required support. The following list includes some typical logistical planning considerations:

- Personnel - The total number and attributes of participants must be determined. This includes the number of protective force personnel or other facility personnel and who they will be (that is, which individuals, shift, and Special Response Team). It also includes the number of adversaries that will be needed and any special qualifications they require. The required number of controllers and evaluators must be determined and their sources decided. Each controller and evaluator must be assigned a position and specific test responsibilities. All participants must be notified of their selection and told when and where to report and what to bring with them. It may be necessary to provide a general notification to all personnel working in the vicinity of the test area.

- Facilities - All facilities necessary for test preparation and conduct must be identified and scheduled. These would include the test area, briefing rooms, weapon and equipment issue, recovery areas, and possibly adversary training areas.

- Equipment - All equipment that is to be used in the test must be identified, the source of each item must be identified, and responsibility must be assigned for providing each item. Normal equipment categories are as follows:

    - Props - Various props are needed for testing purposes. A prop could be almost anything, including false or real badges, simulated explosives, rubber knives, replica weapons, briefcases, furniture, or safes.

- Weapons/MILES/Ammunition - Total numbers and types of weapons, ESS/MILES equipment, and blank ammunition must be determined. Protective force weapons and ammunition are generally limited to what they actually have available. Adversary weapons and ammunition are limited only by the threat guidance, what can reasonably be made available to them, and what they can transport. Any pyrotechnics to be used by controllers must also be identified.

- Duty Equipment - The protective force is limited to their normal duty equipment. The adversaries are unlimited, within reason and current threat guidance. Controllers will need radios, ESS/MILES controller guns, and perhaps flashlights and other items.

- Vehicles - Types and numbers of test vehicles (vehicles that will be used by players or will be in the scenario play) must be determined. Additionally, any vehicles needed for test control purposes must be identified.

- Uniforms and Clothing - The protective force players usually wear their normal uniforms. Adversary uniforms or clothing will depend on the scenario. Controllers/evaluators/observers will be issued some form of distinctive apparel, such as a traffic vest, cap, etc. Weather conditions should be taken into account, and cold weather or rain gear should be available, if needed.

- Special Equipment - Special equipment to be used by the protective force players should be identified and should be limited to such equipment as they normally have available to them. Special adversary equipment needs must generally be identified early, so that equipment can be located and obtained before it is needed.

- Transportation - As necessary, arrangements must be made to transport all test participants to briefing areas, the test area, and the site of their specific assignment. Return transportation needs must also be identified and provided.

- Food/Drink - If the test involves outdoor activity in extreme weather conditions, either hot or cold, plans should be made to provide hot or cold drinks at appropriate places and times. Depending on the time and duration of the test, it may be appropriate to provide box meals to all test participants.

Safety

Safety must be considered during all planning activities. Safety considerations will vary with the type of test activity, but may include general personal safety, weapons safety, vehicle safety, aircraft safety, and availability of medical, fire, and ambulance services.

Every inspection-related performance test that has any safety implications, including most protective force performance tests, requires review by Independent Oversight and approval by DOE field element and/or site safety representatives. The safety representatives should be involved early and throughout the planning process so that potential safety problems can be solved in a timely manner without causing delay or cancellation of the test.

Standard safety plans and risk assessments exist for various types of performance tests, but the standard plans are frequently modified to accommodate the particular test and the site-specific conditions and requirements. Safety plans are developed by the site in accordance with local procedures.

Security
During any performance testing of protective force personnel or equipment, the security of the site must be considered. When personnel or equipment are taken off post or out of service for testing, or when personnel on post are carrying ESS/MILES weapons instead of live weapons, compensatory measures are frequently needed to provide for the minimum security needs of the facility. Any test, even a simple one involving only one or two security police officers on post, may require compensatory measures if the test has the potential to divert the attention of on-duty personnel from their normal responsibilities.

For most performance testing, test subjects are either brought in from off duty for testing, or they are relieved from their posts during the testing period; in these situations, other on-duty personnel provide the needed security. For some tests, such as no-notice tests at entry control portals, any needed compensatory measures would have to be more subtle, to avoid compromising the test element of surprise. For largerscale tactical tests where all normal security posts in the test area are manned by players equipped with ESS/MILES weapons, the common compensatory measure is to place armed shadow force personnel in strategic locations in or adjacent to the test area. Shadow force locations must be off-limits areas, and all shadow force personnel must be under the positive control of a controller at all times.

The need for compensatory measures should be determined by the local operations office. Whether they are employed is a decision to be made by the trusted agent or his/her superiors. However, the Test Director/Exercise Coordinator does have an obligation to raise the question if he/she believes compensatory measures may be required. If compensatory measures are required, the Test Director/Exercise Coordinator has a definite interest in what they are and should be involved in their planning. As with any other planning consideration, the goal for these measures is to affect test realism and safety as little as possible. In this case, however, the final decision rests with the site, and the Test Director/Exercise Coordinator must rely on persuasion, if necessary, to influence a reasonable solution.

PERFORMANCE TEST SAFETY PLAN

I, _____, acknowledge receipt of the attached safety plan. I understand it is my responsibility to become familiar and comply with the contents of this safety plan.

Acknowledgment of the receipt of this safety plan is a requirement to participate in or observe this exercise. This page must be signed and returned no later than _____.

Printed Name _____ Signature _____

Position _____ Date _____

Detection of Contraband and Prohibited Items
(Type of Performance Test)

Ongoing 365 Days per Year; 24 Hours per Day
(Performance Test Date and Time)

Detection of Contraband and Prohibited Items, John Doe
(Safety Plan Name and Person Preparing)

ALL LIMITED SCOPE PERFORMANCE TESTS (LSPT'S) WILL BE CONDUCTED IN CONFORMANCE WITH THIS SAFETY PLAN AND ONLY AFTER SPECIFIC APPROVAL TO CONDUCT THE LSPT'S HAS BEEN GRANTED BY A RESPONSIBLE OFFICIAL. PERSONNEL SERVING AS CONTROLLERS WILL BE FULLY QUALIFIED IN ALL ASPECTS OF THE LSPT.

Scenario:
The ongoing LSPTs are conducted to test the ability of Protective Force (PF) personnel to detect contraband and prohibited items from being introduced into limited areas, exclusion areas, protected areas, and material access areas. LSPTs will be conducted on X-ray machines, metal detectors, and hand and vehicle searches. Security and non-security personnel will try to enter and exit the above-mentioned areas with contraband and prohibited items. Using personnel with whom PF personnel are unfamiliar will ensure credible and realistic test results. The person attempting to introduce the contraband or prohibited item will use only contraband test items that have been approved by the cognizant security authority. Once the entry is initiated, the person attempting the entry will only proceed after being cleared to do so by the security officer conducting the search. The persons attempting the entry will wear clothing that would make the concealment of any weapons on their person virtually impossible, and they will keep their hands open and in plain view at all times. The persons attempting to enter or exit any of the aforementioned areas will strictly follow all instructions given by the controller and obey all instructions given by PF personnel. The controller will announce the LSPT to PF personnel once the contraband or prohibited item has been detected/undetected by the PF. *The sole purpose of the LSPTs is to evaluate the ability of the PF to detect contraband and prohibited items prior to their release into the aforementioned areas. The LSPTs are not designed to test what actions the PF undertakes once they detect or fail to detect the contraband or prohibited item.*

IN THE EVENT OF AN ACTUAL SECURITY ALARM OR SECURITY INCIDENT, THE CONTROLLER WILL IMMEDIATELY ANNOUNCE AND CONCLUDE THE LSPT, TAKE POSSESSION OF THE TEST ITEM/CONTAINER, AND FOLLOW ALL INSTRUCTIONS ISSUED BY PF PERSONNEL.

Requirements:

1. Controller
2. Person to carry contraband or prohibited item into the area
3. Contraband and prohibited item(s)
4. Support items, such as lunch boxes, purses, notebooks, gym bags, vehicles.

PF Response:

_____ Yes _____ No

If a no-notice PF response is desired, check the following measures being taken to ensure safety during the response.

____ Drill announcements will be made on all PF networks immediately after PF response is initiated, and periodically thereafter.

____ Controller is located in the PF Central Alarm Station (CAS).

____ The PF is informed that an exercise will take place and that they are to follow the safety and health requirements contained in this plan and in the site procedures. This instruction will be provided by site representatives briefing the PF prior to the shift during which the performance test will take place.

____ Controllers are located at the exercise location.

If PF response is not desired, check those measures being taken to preclude response.

____ Prior notification of CAS.

____ Prior notification of PF.

____ Presence of non-playing PF personnel briefed on the scenario at the performance test location. Controller located in the CAS. A second controller will be located in the CAS with a final approved copy of this LSPT Safety Plan and LSPT Safety Briefing. This controller will be able to provide positive identification of the onsite controller and any support personnel participating in the LSPT. The onsite controller will ensure that the CAS controller is physically located in the CAS prior to departure for the area in which the LSPT will be conducted.

____ Controller located in the immediate vicinity (within sight and hearing of the PF and support personnel) of the LSPT.

List other specific safety measures below:

1. All personnel attempting to gain entrance into one of the identified areas will be briefed on the LSPT objectives and how they should conduct themselves during the LSPT.
2. All contraband or prohibited items will be photographed prior to the initiation of the LSPT.
3. All personnel attempting to gain entry or exit with contraband items will be photographed prior to the initiation of the LSPT.
4. All personnel attempting to gain entry or exit with contraband or prohibited items will be instructed to keep their hands in plain view, not to make any sudden moves, and comply with all instructions given by PF personnel.
5. Only epoxy–encased, cognizant security authority-approved test weapons will be used in LSPTs requiring weapons.
6. All support personnel attempting to gain entrance or exit with contraband or prohibited items will be briefed and required to read and sign the attached rules of exercise.

Performance Test Boundaries:

____ Applicable

The immediate area of the security post where the LSPT is being conducted.

____ Not applicable

If applicable, describe the performance tests boundaries and the restrictions on performance test participant movements in detail:

Off-Limit Areas:

____ Applicable

____ Not applicable

If applicable, describe the off-limit areas and how they will be designated:

Safety Equipment:

____ Controller Radios

____ PF Radios

____ Orange Vests

____ "Glow Sticks"

____ First Aid Kit

____ other required safety equipment:

Specific Safety Hazards not Covered Elsewhere:

____ Applicable

____ Not applicable
These LSPTs are being conducted with armed PF personnel. As with all such exercises, the remote possibility exists that weapons may be drawn if the exercise plan is not adhered to, or if PF personnel are not properly trained. However, because of the constraints placed upon the exercise controllers by this plan and the level of preparation of the participants, the level of risk is actually below that experienced during normal day-to-day operations.

Radiation Safety Provisions:

____ Applicable

____ Not applicable

If yes, check those applicable to this LSPT:

____ Personnel participating in the LSPT have been briefed concerning radiation safety requirements for the area with which the LSPT will be conducted.

____ Personnel will be continuously escorted while in the radiation areas in which the LSPT will be conducted.

List any other specific radiation safety provisions for this LSPT:

Personnel Assignments (list below):

The names of the controllers and the person carrying the contraband or prohibited items will be filled in prior to conducting the LSPT.

Protective Force Appendix Required:

____ Yes

____ No

DOE Safety Review:

List any pertinent safety procedures concerning this LSPT that are not addressed in this plan. Normally, the PF will not be notified in advance of the specifics of the LSPT being conducted. The shift captain will be notified upon termination of the LSPT.

APPROVALS:

_____ Date _____
Director, Cognizant Security Authority

_____ Date _____
Safety and Health Representative

SAMPLE PERFORMANCE TEST PLAN

OBJECTIVE: This performance test is designed to

1. Test individual employee response to finding an unattended Secret Restricted Data (SRD) document
2. Verify compliance with the notification process to Classified Document Control Office (CDCO)
3. Verify PF compliance with the procedure for responding to this incident.

SCENARIO: A simulated SRD document will be left unattended in an area accessed by "L"-cleared employees. This document will be marked as a formal SRD document. Personnel recovering and responding to the simulated classified document shall have no indication that the contents of the document are actually unclassified.

EVALUATION CRITERIA:

1. A simulated SRD document consisting of approximately five pages of unclassified text and drawings shall be placed on the table next to a copy machine located in Building xxx, Room xxx. The document shall be placed in the designated location at approximately 7:30 am.

2. Upon notification of the unattended "classified" document, the CDCO will verify that the individual finding the document completed the following actions (answers will be based on applicable procedures):

   a) xxx
   b) xxx
   c) xxx

3. The Document Control Center shall also verify that the PF completed the following actions (answers will be based on applicable procedures) :

   a) xxx
   b) xxx
   c) xxx

4. In order to successfully complete the performance test, the following must occur:

   a) Classified Document Control Office is notified within three hours of placement.
   b) Individual locating the unattended document adheres to all protection and notification requirements.
   c) PF officer responding to the incident adheres to all protection and notification requirements.

TEST CONTROLS: The following controls will be adhered to during conduct of this performance test.

- Only self-assessment team members involved with the conduct and evaluation of this performance test will be made aware of all information surrounding the conduct of the test.
- There are no additional safety requirements for this performance test. All current facility safety requirements will be adhered to during this performance test.
- This will be a no-notice exercise; therefore, the organization being assessed will not be given any information regarding the conduct of this performance test prior to the test.
- The simulated SRD document used during this exercise will consist of an unclassified document marked at the SRD level with all appropriate markings and covers. There will be no indications to a casual observer that the document is not classified.

RESOURCE REQUIREMENTS: The following resources are needed to conduct this performance test.

- Simulated SRD document
- Identified location to place the document
- Three self-assessment team members to be assigned the following:
  a) Monitor the document
  b) Monitor the PF response
  c) Monitor the CDCO

TEST COORDINATION REQUIREMENTS

No coordination requirements are necessary since this is a no-notice exercise. Team members monitoring the various aspects of the performance test will identify themselves to participants only when it becomes necessary.

OPERATIONAL IMPACT(S) OF TESTING PROGRAM

Since this performance test is being conducted during normal duty hours, there will be no need for additional funds for overtime payments, and there is no expectation of a loss of productive time for personnel who will be participating in the exercise.

COMPENSATORY MEASURES

There are no compensatory measures required for the conduct of this exercise.

COORDINATION AND APPROVAL PROCESS

The following steps and documentation will be followed in the conduct of this exercise.

- This test plan will be approved by the self-assessment team lead prior to the conduct of the performance test. Approval of this test plan will be documented by the team lead's signature and date on this test plan.
- A participant log containing name, job title, organization, telephone number, and date will be completed by all participants of this exercise.
- A data collection form containing the date, performance test type, name of evaluator, and chronological description of actions observed will be completed by all assessment team members participating in the evaluation of this performance test.

REFERENCES: The following references will be used in the conduct and evaluation of this performance test.

- DOE O 471.6, Information Security Program
- Information Security Standard Operating Procedure #
- PF Standard Operating Procedure #

TEAM LEAD: _____ Date: _____

NO-NOTICE PERFORMANCE TEST: BEST PRACTICE

Date: August 5, 2013

Site: Nevada Field Office (WSI Nevada)

SECLL Title: No-notice Performance Tests **SECLL Identifier:** SEC-WSI-NV-08-05-2013

Document Type: Best Practice

Lessons Learned Statement: Prior to developing any no-notice performance test, we met with our protective force leadership, safety, VA lab, and performance testing. As a group, we discussed what objectives each wanted from the performance test. We agreed that the primary objective was to validate the ability of the Protective Force to identify and locate an unauthorized individual(s) within a specific Area of Operation, with a secondary objective of the Protective Force's ability to respond to a low level threat (Protester). Safety was the primary concern associated with this type performance test. The group evaluated various pathways and determined the areas which present significant safety concerns. Each concern was addressed and mitigated with specific hazard controls.

Discussion: Performance test plans were developed with emphasis on pre-operations and actual conduct of the performance test. Each phase is described below.

A. Pre-conduct operations

1. Test Administrator will meet with the site tactical commander prior to him/her assuming their shift, advise him/her of their Trusted Agent responsibilities and brief him/her on the test time and guidelines of the performance test. (Recorded on briefing checklist.)
2. Test participant(s) will carry nothing other than a cell phone while performing this performance test.
3. The test participant(s) will wear normal site attire. Under no circumstance will he/she/they wear clothing that can be misconstrued as that worn by an adversary (e.g. dark or camouflaged).
4. The site tactical commander will confirm with the Test Administrator that he/she is in the Central Alarm Station (CAS) prior to arriving at the performance test start point

B. Conduct

1. The site tactical commander will confirm with the Test Administrator, (or designee) that he/she is in the CAS and ready to conduct the performance test.
2. The test participant(s) will enter the area of operation from a predetermined location.
3. The test participant(s) will proceed directly to the exterior PIDAS fence.
4. At no time will the test participant(s) walk in the direction of or approach a TRT Unit.
5. If the test participant(s) are challenged and an escalation of security phase is initiated, the statement will be announced over the Protective Force radio net, the ESS radio net, and the DAF Public Address System: ***" This a Protective Force No-notice performance test. Only Protective Force personnel are involved in the test. All others will continue with normal operations."***
6. If the test participant(s) reaches the exterior PIDAS fence unchallenged, he/she/they will continue to make noise and attempt to draw attention to their location.
7. If the test participant(s) remain unchallenged, he/she/they will enter the PIDAS, ensuring the gate is locked behind them and proceed directly to the interior PIDAS fence. Once at the interior PIDAS fence, he/she/they will tug on the taut wire with no more force than to set the

alarm off.
8. The test participant(s) will back away from the interior PIDAS fence, ensuring his/her/their hands are clearly visible.
9. The test participant(s) will remain away from the interior PIDAS fence; at no time will any threatening gestures be made towards the protective force.
10. **If the test participants are detected prior to reaching the PIDAS but are not located by the Protective Force, the test participants will standup and don their reflective safety vest if a protective force vehicle comes within 25 yards (75 feet) of their position**.
11. The test participant(s) will comply with all directions/orders given by the Protective Force.
12. The site tactical commander will maintain control of the performance test and will terminate it if at any time he/she feels it necessary. Termination of the performance will occur if a real world security phase is initiated for other reasons
13. The site tactical commander is the only individual authorized to terminate the performance test. The test participant(s) will carry a "Trusted Agent" identification card identifying him/her/them as a participant in a performance test.

Analysis: The first thing we discover was there is no way to conduct a complete no-notice performance test. There must be someone in the Protective Force chain of command that can control the performance test and stop it should things get out of hand. We selected the site tactical commander to be that individual. Our first attempt at no-notice performance testing was somewhat disconcerting; however, you have to trust in the training that our Security Police Officers receive. Most of our no-notice performance tests are directly tied to the Low Level Threat. However, we have expanded our no-notice performance testing program to included explosive detection and active shooter scenarios

Recommended Actions: None

Priority Descriptor: Routine

Topical Area: Program Management Operations

Sub Topical Area: Performance Assurance Program

Estimated Savings: N/A

Keywords: No-notice Performance Testing

Reviewing Official: WSI Nevada

Derivative Classifier: WSI Nevada

CRITICAL ASSET IDENTIFICATION PERFORMANCE TEST

Objective: To evaluate critical asset identification capabilities of individual PF personnel.

Scenario: Protective force personnel are required to identify photographs of authentic critical assets, which are intermingled among numerous other photographs of spurious nuclear weapons components, nuclear devices, SNM, or other material resembling critical assets stored at the respective site. The test should not be limited to identification, but should also require personnel to identify likely storage locations and indicators for unauthorized movements/shipments of critical assets.

Evaluation criteria:

1. Are protective force personnel able to quickly identify critical assets?
2. Are protective force personnel familiar with likely storage locations of critical assets?
3. Are protective force personnel able to identify indicators of unauthorized movements/shipments of critical assets (e.g., lack of specified paperwork or dispatch to a particular type of alarm)?

Safety plan: A safety plan will be completed for this performance test.

Commentary

This test is relatively simple to organize and administer. The primary difficulty encountered is displaying all photographs in a manner that does not indicate which photographs are false. This difficulty is compounded by the fact that many photographs of critical assets may be classified. One method of circumventing this obstacle is to place all photographs in identical document protectors, place opaque tape over portions of the document protector where classification markings are visible. This performance test may be employed as part of a larger "shift readiness" performance test, which typically includes numerous, easily administered performance tests where a representative sample of the protective force is selected for participation.

DURESS RESPONSE TEST

Objective: To determine whether the CAS operator is able to perform required response functions and whether the protective force can conduct an effective response, using sound individual and team tactics.

Scenario: The assessment team initiates a no-notice duress test by having an on-duty SPO activate his duress instrument because he feels faint and is about to pass out. Receipt of the duress alarm, reporting, and dispatch of protective forces will be monitored at the CAS. Actions of the responding forces will be evaluated at the scene.

Evaluation criteria:

1. Is the CAS being properly monitored?
2. Is dispatch of security patrols prompt?
3. Are protective force communications effective?
4. Are proper individual and team tactics demonstrated?

Safety plan: A safety plan will be completed for this performance test.

Commentary

Properly conducted, even a small-scale, limited-resource duress response test can yield data on a wide range of areas such as command and control; alarm station operation; individual tactics; team tactics; communications; and observation, assessment, and reporting. The use of an on-duty SPO obviates the need for additional role players, yet gives responders something concrete to assess (for example, do they observe the SPO slumped at his post, do they attempt to raise him on the radio, what conclusions do they draw?). Depending on response procedures at the site and additional scenario inputs, the test can also drive a broader range of tactical actions.

It is vital to stress that both the initial duress alarm and all subsequent communications be accompanied by appropriate notification that these are exercise-related activities. It is also necessary to ensure that appropriate response exercise safety procedures be carefully reviewed for each oncoming shift during the period in which test exercises are to be conducted.

ENTRY/EXIT SEARCH OF HAND-CARRIED PARCELS TEST

Objective: To evaluate the SPO's ability to conduct an effective search of hand-carried parcels while processing pedestrian access.

Scenario: The assessment team places items of contraband, simulated classified information, and metal objects configured to represent SNM or instruments of sabotage in briefcases, lunch pails, and other handcarried containers. These will be carried by badged employees attempting to enter or exit appropriate security areas. The inspection team will observe the parcel search actions of the SPO during this attempt.

Evaluation criteria:

1. Does the SPO understand the procedures governing search of hand-carried parcels?
2. Does the SPO make proper use of available search equipment (X-ray or metal detectors) as specified in post orders?
3. Is the SPO capable of conducting an effective search of a hand-carried parcel?
4. Does the SPO understand the correct actions to be taken and notification to be made when discovering:
   a. Contraband
   b. Classified information
   c. SNM
   d. Weapons or explosives

Safety plan: A safety plan will be completed for this performance test.

Commentary

Most of the considerations discussed under identification of personnel test also apply to the personnel search tests. In addition, great care must be exercised to ensure that when the simulated prohibited item used might represent an immediate threat to the protective force personnel on post (e.g., a weapon or explosive device), that the test itself is halted *as soon as the item is detected*. Once the SPO has been informed that a test has taken place, he/she may be allowed to continue with the notification portions of the test.

USE OF FORCE, APPREHENSION, AND SEARCH

Objective: To evaluate the ability of SPOs to apply DOE policy on the use of force in practical sitespecific scenarios; additionally, to evaluate the application of self-defense, subject control, and arrest techniques.

Scenario: A representative sample of SPOs is selected for this test. These personnel will receive a detailed briefing, which will stress adherence to safety procedures and the limitations governing the application of physical force during these tests. In particular, the briefing will stress the special safety prohibitions that will govern scenarios in which the baton might be drawn. A non-firing exercise handgun will be substituted for the SPO's service weapon during the performance test.

SPOs will encounter a variety of situations in an office building requiring them to take action and apply some degree of force, up to and possibly including deadly force, to resolve the situation. The scenarios may include an altercation among employees, theft of classified documents, burglary, intoxicated or psychologically disturbed employee, and/or suicidal employee. The scenarios will be played by CAT members. SPOs will be required to demonstrate a range of self-defense, subject control, and arrest techniques. SPOs may also be required to draw a baton or a non-firing exercise handgun, substituted for their service weapon.

Evaluation criteria:

1. Does the SPO apply only the amount of force necessary and in compliance with DOE policy to resolve the situation while protecting his/her life and the lives of others?
2. Does the SPO identify and preserve items of evidence?
3. Does the SPO demonstrate proper techniques for approaching, handling, and controlling hostile and non-hostile subjects?
4. Does the SPO use proper self-defense techniques?
5. Does the SPO use proper arrest and search techniques?

Safety plan: A safety plan will be completed for this performance test. This plan will incorporate special controls upon the application of physical force in contact situations.

Commentary

This test may be repeated with variations to test many different responses. The variations are introduced by having role players respond in different ways during the scenarios. Great care must be given in coaching the role players to perform in ways that will elicit the desired responses. Great care must also be taken to ensure that role players do not offer levels of resistance that could lead to uncontrolled grappling, with its attendant risk of injury; therefore, role players will become passive during actual physical contact, allowing themselves to be controlled and handcuffed. This "passive role" must be written into the test plan and safety plan, and role players must be fully briefed on the limitations on level of resistance. This issue must also be addressed thoroughly in briefing protective force participants prior to initiating the scenarios. Again, it should be emphasized that the focus of these drills is on the selection of the right techniques and levels of force. Tests of the SPO's actual ability to fully apply restraint techniques must be conducted only in an appropriate training environment, with proper safety equipment and a qualified sparring partner (typically, the site's own self-defense instructor).

In addition to providing data in this area, these exercises provide useful information on areas including individual and team tactics, and observation, assessment, and reporting. This latter area can be served by having each participating SPO complete a protective force standard incident report at the scenario site. A comparison of this report with the actual events observed by controllers during the scenario yields data concerning the SPO's ability in this area.

COMMAND AND CONTROL TABLETOP EXERCISE

Objective: To evaluate the notional command and control capabilities of protective force supervisors and other first responders to direct assets and implement site plans for a given security incident.

Scenario: Tabletop participants selected for testing usually include a representative sampling of shift supervisory personnel, CAS operators, and other key first responders who may be working on any one given shift. Testing is conducted in a notional tabletop forum, where participants are arranged around a sand table mock-up of site facilities and/or detailed facility maps. An inspector begins by providing participants with a detailed scenario briefing for a chemical attack, recapture/recovery of SNM, emergency evacuation, or similar incident. The briefing should be configured to include types of alarms that have been communicated by the CAS and other pertinent environmental descriptors that require an escalating level of response. As the scenario unfolds, participants are shown various photographs or provided with key elements of information that would involve specific response actions noted in site incident response plans.

Participants should be permitted reasonable amounts of time to utilize appropriate plans, procedures, and documentation while articulating response actions, issuing orders, making notifications, simulating the deployment of an entire protective force shift, and requesting information and intelligence, as appropriate. Facility maps or a sand table mock-up should be utilized to illustrate each participant's response actions.

Evaluation criteria:

1. Are participants able to quickly articulate required/appropriate response actions?
2. Are participants familiar with associated plans, procedures, and memoranda of understanding?
3. Are participants able to collectively execute response plans and/or formulate appropriate solutions?

Safety plan: A safety plan need not be completed for this performance test.

Commentary

This test may be repeated with scenario variations to test many different responses. Reviewing a variety of response procedures and vulnerability assessments, and identifying specific actions required for a given incident will assist in the development of challenging scenarios. Great care should be given to inconspicuously prompt participants to act upon the desired scenario inject. A comparison of test results with the actual events observed by controllers during the force-on-force exercise yields valuable data concerning the overall command and control capabilities of the protective force.

ACCESS CONTROL

Objective: The objective of this test is to determine whether an individual could access a security area with either an old badge or with no badge.

Scenario: The assessment team member, with a site representative, will attempt to enter a security area where access is controlled by either a Security Officer (SO) or receptionist. The team member will have an old badge or will conceal his/her badge before attempting entry.

Conditions: Normal operating conditions.

Evaluation Criteria: The SO or receptionist shall challenge the team member, and deny access until a positive identification is made.

INTRUSION DETECTION AND ASSESSMENT SYSTEM: SECURITY LIGHTING

Objective: The objective of this test is to determine if adequate security lighting has been provided at all security areas, for the assessment of alarms, detection or unauthorized personnel attempting access, and to properly check credentials.

Scenario:

Procedures:

a. The test will be conducted approximately one hour after sunset.
b. The site representative will provide a calibrated light meter that displays light levels in foot-candles.
c. Light-level readings will be taken within the perimeter intrusion detection and assessment system (PIDAS) zone along the centerline of the zone, along the outer fence, and along the inner fence. Along each line of measurement, readings will be taken at 25 foot intervals between the light fixtures.
d. Light-level readings will be taken around PF posts out to 30 feet from the post. Additional readings will be taken out to 150 feet from the post.

Conditions:

The test will be conducted during non-operational hours, when the security lighting is activated. All light fixtures should be functioning properly.

Evaluation Criteria:

1. Lighting must be at least 2 foot-candles within 30 feet of entry control points for personnel to check credentials.
2. Lighting must be at least 0.2 foot-candles within 150 feet of PF Post for unaided assessment of alarms by PF.
3. Lighting for PIDAS zones must be at least 0.2 foot-candles to allow the PF to assess alarms using closed-circuit television (CCTV).
4. All lighting must meet the requirements outlined in DOE directives.

Test Results:

All evaluation criteria must be answered "yes" to pass the test.

1. Lighting is at least 2 foot-candles within 30 feet of entry control points for personnel to check credentials.
2. Lighting is at least 0.2 foot-candles within 150 feet of PF Post for unaided assessment of alarms by PF.
3. Lighting for PIDAS zones is at least 0.2 foot-candles to allow the PF to assess alarms using CCTV.
4. All lighting meets the requirements outlined in DOE directives.

INTRUSION DETECTION AND ASSESSMENT SYSTEM: BALANCED MAGNETIC SWITCHES (BMS) SENSORS

Objective: The objective of this test is to determine if door mounted balanced magnetic switch (BMS) can be moved more than one inch (measured from the leading edge of the door to door frame) without indicating an alarm condition.

Scenario:

1. The assessment team member will select ___ BMSs to test.
2. The assessment team member and site representative will proceed to the selected alarm location(s) equipped with a PF) radio.
3. The CAS will be notified to announce when the alarm is received. When the alarm has been received the test is complete for that sensor.
4. The assessment team member will observe as the site representative attempts to open an alarmed door, a distance greater than one inch, without causing an alarm.
5. The assessment team member will ensure that the BMS is moved slow enough to allow the CAS to detect and announce the alarm.

Conditions: This test will be conducted during operational or non-operational hours depending on location of test and impact on operations.

Evaluation Criteria:

1. Ensure an alarm signal is received by the CAS.
2. The BMS must sound an alarm prior to being opened greater than one inch.
3. Ensure that the CAS receives the alarm and that it has an individual address and is not part of a loop of alarms.
4. Ensure maintenance records reflect proper maintenance.
5. Ensure that a record of previous tests exists and that the tests were performed in accordance with established procedures and time frames.

EXTERIOR PERIMETER SENSORS

Objective:
The objective of these performance tests is to determine the effectiveness of exterior perimeter sensors.

System Tested:
System: Intrusion-detection system

Function: Perimeter-intrusion detection

Component: Exterior sensors, transmission lines, alarm processing equipment, interfaces with closed circuit television (CCTV) and central alarm station (CAS) operation, testing and maintenance of perimeter sensors.

Scenario:
Assessors should select one or more zones of a perimeter system for testing based on sensor configuration, terrain, location of buildings and portals, and operating history. A quick tour around the perimeter is helpful in identifying zones and potential deficiencies. Items of interest may include ditches, humps, dips, other terrain variations, obstacles or obstructions, sewer lines, pipes or tunnels that pass under the zone, piping or utility lines that pass over the zone, barriers that could be used as a platform to jump over sensors or to avoid observation, excessive vegetation, and standing water. Particular attention should be paid to the identification of potential gaps in sensor coverage.

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

- At least two zones should be tested. If the zones employ different sensor configurations, or if the sensor configuration at portals is significantly different, the inspectors should consider selecting at least one of each type.

- At least one of each type of sensor should be tested, if possible. This should include sensors on building roofs and sensors (if any) in tunnels under the perimeter.

- If the first few performance tests do not indicate problems and there is no evidence of exploitable deficiencies, the assessors should not generally devote extensive time to testing numerous zones and sensors. However, if deficiencies are apparent, the assessors should collect sufficient data to determine if a deficiency is an isolated instance or evidence of a systemic problem.

- Tests should be conducted for selected zones in which terrain features or questionable installation practices are likely to degrade detection capability.

It is useful for assessors to observe security alarm technicians or security police officers (SPOs) conducting routine operational or sensitivity tests. Assessors should determine if the tests, calibrations, and maintenance procedures are consistent with DOE orders and the SSSP, and if they are an effective means of testing the systems. Two goals are accomplished by having the facility's security technicians conduct the routine test prior to testing by the inspectors. First, the facility tests are indicators of the effectiveness of the test and maintenance program and procedures. Second, the facility tests should verify that the sensors are calibrated according to facility specifications, thus the assessors will be testing a system that is operating as the facility intends. This may be important in identifying the root cause of any deficiency.

The assessors may conduct walk tests, crawl tests, run tests, jump tests, climb tests, and step tests, as appropriate, to determine whether an adversary could cross the perimeter without detection and whether the individual sensors are properly calibrated.

Assessors should monitor the alarm annunciation in the CAS and secondary alarm station (SAS) to determine whether the alarms are functioning properly. The assessors may also observe the operation of interfacing systems, such as the automatic CCTV display and video recorders.

Evaluation:

If the detection system is effective, the sensors will detect intrusion and the alarms will annunciate accordingly.

FENCE DISTURBANCE SENSORS

General Characteristics: Sensing wires/cables attached to or woven through fence, sonic capacitance, or piezoelectric technologies

Intruder Detection Capabilities: Cutting, climbing, or other vibration/deflection of sensor wire or fence

Vulnerabilities: Tunneling, trenching, bridging

Concerns:

- Fence disturbance sensors are susceptible to defeat by tunneling, bridging, or jumping, if no physical contact with the sensing wires occurs.

- Depending on the sensitivity setting, fence disturbance sensors may be susceptible to high false alarm rates. Common causes of false alarms include high winds, animals, and other sources of fence vibration. It is important that fences, gates, outriggers, and barbed wire be mechanically sound and well maintained to prevent excessive fence vibration.

- In some sensor designs, the sensing wires are least sensitive near the terminal connections and corners.

- The sensor wire or sensors must contact the fence for reliable, nuisance alarm-free performance. It is important that the sensors and/or cabling be attached per manufacturer specifications.

Types of Tests:

- Unaided Climb Test: The test consists of an individual (preferably a small individual) climbing the fence at various locations to verify that detection occurs. Attempts should be made near fence posts, especially corners/posts.

- Ladder Climb Test: A ladder is placed against the fence. An individual climbs the ladder to the point of sensor activation.

- Cutting Attack: No actual cutting of the sensor wires or fence fabric should be performed.

- Jump Tests: These tests cannot normally be conducted if a fence disturbance sensor is properly installed, due to the height of the detection zone (eight feet or more). However, adjacent structures used as platforms may permit an individual to jump over the fence/sensor wire, if personal safety can be ensured.

Test Guidelines:

- All of the unaided climb tests should be conducted on several fence posts in at least two typical zones.

- Zones that are substantially different (gates or different sensor configuration) should also be considered for testing.

- Areas that appear vulnerable to jumping should be tested to determine whether vulnerability exists. Safety concerns should be addressed.

- If an individual sensor can be defeated, that same sensor should be tested again to determine whether the deficiency can be repeated. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit the sensor deficiency.

- If an individual zone can be defeated, other zones should be tested using the same methods to determine the extent of the problem. The assessors should conduct several (three to five) more tests in different zones. If most of these tests indicate that the sensors can be reliably defeated, it is likely that there is a systemic problem. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, additional testing should be considered. Rarely would an assessor test more than 10 to 15 zones using the same methods.

- If the adversary has sufficient knowledge, time, and equipment, bridging or tunneling techniques can defeat all fence disturbance sensors. Such tests should only be conducted if a zone is particularly vulnerable (for example, due to barrier placement), or if patrol frequencies and direct visual observation (CCTV or from guard posts) are considered inadequate to provide reasonable assurance that such attempts are detected.

FENCE DISTURBANCE SENSORS: EXTERIOR PERIMETER INTRUSION-DETECTION SYSTEM

Interview Items

Installation location:

Operational test frequency:

Operational test method:

Sensitivity test frequency:

Sensitivity test method:

Acceptance criteria for sensitivity test:

False alarm history/records:

Make/model:

Measures to prevent erosion:

Tamper switches (transmitter, receiver, junction boxes):

Tour/Visual Inspection Items

Vegetation present?

Zone length OK?

Complements other sensors?

Overlap sufficient?

DATA COLLECTION SHEET: FENCE DISTURBANCE SENSORS
EXTERIOR PERIMETER INTRUSION-DETECTION SYSTEM (PIDAS) TEST METHOD

Zone tested	Unaided Climb	Ladder Climb	Cutting Jump
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Comments:

INTERIOR SENSORS

Objective: The objective is to test the effectiveness of interior sensors in detecting adversary intrusion.

System Tested:
System: Intrusion-detection system

Functional Element: Interior intrusion detection

Component(s): Interior sensors, transmission lines, alarm processing equipment, interfaces with CCTV and CAS operation, testing and maintenance of interior sensors.

Scenario:
The assessors should select several interior locations (material access areas, vaults, vital areas, or vault-type rooms) for testing, based on a number of factors: sensor types used, construction type, materials, configuration of the interior area, and operating history of the various sensors. At least one of each type of room or vault configuration and sensor should be tested.

The assessors should review building layouts and architectural drawings. They should also briefly tour the facility to familiarize themselves with typical protection system configurations and to identify potential weaknesses. The relationship between sensor application and the types of structural barriers in use should be noted. The detection capabilities of individual sensor types may vary depending upon the types of barriers used and the ability of these barriers to resist or delay penetration. Also, since some sensors respond to physical attacks on the barrier material, it is important that the detection technology employed (for example, acoustic, vibration, strain, or capacitance technologies) be suited to the barrier material used.

In general, sensors will be of three generic types: motion (or area), barrier penetration, and proximity. Each of these types is subject to various physical and environmental limitations that must be considered when assessing suitability and operating performance. Limitations involve electromagnetic, radiological, acoustical, seismic, thermal, and optical effects, as well as the physical limitations imposed by equipment placement, room arrangement, and building materials used in walls, ceilings, floors, windows, doors, and penetrations (for example, ductwork and cable chases).

If possible, the assessors should observe alarm technicians or SPOs during the conduct of routine operational and sensitivity tests of selected sensors. The assessors should base their selection of the sensors to be tested on the number, type, configuration, and operational history of those sensors. During this portion of the test, inspectors should observe calibration and maintenance procedures to determine whether they are consistent with DOE orders and approved SSSPs. In addition, observation of these tests may indicate the effectiveness of the test and maintenance program. Observations of facility-conducted tests are helpful in identifying the root causes of many noted deficiencies.

The assessors should conduct standard walk tests and tamper-indicating tests (provided no physical damage to the sensor will result) for each motion detection (area type) sensor tested. Barrier sensors (magnetic switches, glass sensors, and capacitance devices) and proximity sensors may require other tests as applicable and as identified in manufacturer's instructions. The purpose of these tests is to determine whether each sensor type is functioning, whether it can detect attempted tampering, and whether it can detect its design basis target (intruder) or activity (for example, attempted barrier penetration using force or attack tools).

Within a single area, there may be several types of sensors that have different detection goals. For example, some barriers may have a penetration detection sensor, a volumetric area sensor for the interior, and a proximity or capacitance sensor to protect the actual item.

The assessors should monitor the alarm annunciation in the alarm stations. They should also observe the operation of any interfacing systems, such as CCTV displays and video recorders, to determine proper functioning.

The number of areas and sensor types to be tested depends on the available time, importance of the system in the overall protection program, and operating history. The following guidelines are intended to assist the assessor in selecting areas and sensors for testing:

- At least five protected interior areas (rooms/vaults/material access areas) should be tested. Priority should be given to those areas containing the most critical assets.

- At least one of each type of sensor should be tested, if possible, including motion sensors, penetration sensors, and proximity sensors, if used.

- If several tests of the same type of sensor are satisfactory, extensive testing of that sensor in different areas is not necessary. However, if deficiencies are apparent, sufficient testing should be conducted to determine whether there is a systemic weakness.

- Tests should be conducted for selected areas where environmental concerns (noise, electromagnetic interference, temperature, and humidity changes) or physical obstructions are likely to degrade sensor performance.

Evaluation:
If a detection system is to be effective, the sensors must detect intrusion, the alarm condition must be correctly assessed, and protective forces must be available for a timely response.

Assessing Sensor Performance:
The primary objective in evaluating interior intrusion-detection sensors is to determine whether they effectively detect penetration, intrusion, or proximity to protected devices or equipment. Other factors to consider are:

- Do balanced magnetic switch (BMS) sensors initiate an alarm when exposed to an external magnetic field or when the switch is moved one inch from the magnet housing?
- Does the sensor layout allow adversaries to circumvent any sensor(s) because of alignment, obstructions, or environmental interference?
- Are there any temporary entry points or penetrations to barriers that could allow undetected intrusion?

Interpreting Results:
The following guidelines are provided to assist the assessor in interpreting evaluation results.

- Many interior sensor systems employ redundant or layered protection schemes that rely on a combination of barrier, volumetric, and point protection systems. If any one of these is found to be deficient during testing, this finding should be evaluated in the context of the site-specific protection program objectives and the effectiveness of other complementary systems.

- In some cases, facility tests may indicate sensors are properly calibrated but inspector tests may indicate that the sensors can be defeated or cannot reliably detect intrusion. In such cases, the inspector can reasonably conclude that there are deficiencies in the test and calibration procedures or in the quality assurance program, or both.

- When facility tests and calibrations and the tests conducted by inspectors indicate that sensors are performing according to specifications, the limitations of the test procedures used must still be considered. All modes of defeat and all physical and environmental factors may not have been considered when conducting the tests.

- Sensor performance that does not appear to be in accordance with specifications may simply indicate sensor drift or an alignment problem. However, a systemic deficiency in sensor design, application, or maintenance might also be indicated. If the facility tests indicate that sensors are out of calibration, inspectors should consider instructing the facility's technicians to test a representative sample of sensors to determine the extent of the problem.

Special Considerations:
Some sensors are sensitive to the size of the intruder. The assessor should request the facility to provide a small person to conduct walk tests. If special equipment is necessary, it should be provided. Often, interior sensors may be located at ceiling height or in relatively inaccessible places (for example, in ductwork or cable chases). Ladders or other aids may be needed.

Related testing or activities, such as those for barriers, card access control systems, CCTVs, or line supervision or tamper indication, are typically conducted concurrently with sensor tests in order to minimize data-collection activities.

PERIMETER CCTV TESTING & LONG RANGE CAMERA/TRACKING SYSTEMS

System Description: Fixed and PTZ cameras, usually with low-light capability, mounted on pole, tower, or wall; coaxial, fiber optic, cable or microwave transmission; associated switching, display, and recording equipment.

Capabilities: Perimeter surveillance and intrusion assessment with ability to discriminate human intruders from animals or other causes of false or nuisance alarms from the perimeter intrusion-detection system.

Vulnerabilities: Extreme weather (ice, snow, fog, rain, wind), inadequate security lighting, improper alignment or overlap, and visual obstructions or shadows caused by structures or uneven terrain.

Concerns:

- Cameras and associated supporting systems (switches, monitors, and recorders) are complex devices requiring extensive maintenance and calibration. Certain components (especially camera image tubes) are subject to predictable failure due to age, which may be a system-wide occurrence.
- CCTV capability may be seriously degraded by weather extremes (ice, fog, snow, rain, wind-blown dust). Where extremes are prevalent, environmental housings (blowers, heaters, wipers) should be present and in good working condition.
- If CCTV towers, poles, or wall mounts are not rigid, the cameras are subject to wind-induced vibration, which can cause loss of video assessment capability.
- For outdoor application, cameras should have a broad dynamic range to allow for effective operation during daylight and darkness. Light-limiting and auto-iris capabilities should be provided to compensate for varying background light levels and to minimize "bloom" from bright light sources (perimeter lighting, vehicle headlights).
- Visual obstructions (buildings, vegetation, towers, fences, structures, or terrain irregularities) can block camera fields of view, creating the potential for intruders to hide or to cross the isolation zone without being observed. The shadows from such obstructions can also interfere with effective observation.
- Camera image tube and video monitor burn-in can result from constant focus on a high-contrast background (extreme light-to-dark ratio), which degrades camera and video monitor performance.
- If camera placement or alignment is improper, there may be "holes" in the CCTV coverage that permit an unobserved intruder to cross the isolation zone. Additionally, if the field of view of the camera is too long for the camera lens, an intruder at the extreme end of the field of view may not be adequately observed. (Note: Industry requires that the postulated adversary occupy at least five vertical scan lines when standing at the far end of the camera's field of view.)
- If cameras are located outside of Protected Area boundaries (to provide better coverage within intrusion-detection system zones), they may be more vulnerable to tampering.
- Automatic camera call-up on the alarm monitor at the CAS/SAS, upon activation of an intrusion detection system sensor (if employed), should be sufficiently rapid to observe the intruder before he/she crosses the isolation zone and reaches the inner perimeter fence. Alternatively, the video recording system (digital or laser disk) should be capable of recording and playing back the camera scene showing the intruder crossing the isolation zone.

- PTZ cameras should have limit switches to preclude their facing directly into bright light sources. Also, if they are called up by intrusion-detection system activation, they should be programmed to automatically position themselves to view the area from which the alarm was received.

Types of Tests:

Functional Test
A functional test of each camera should be performed from the CAS/SAS by calling up each camera scene to verify that cameras are operating and that a clear image is received. If multiple monitors are used for continuous display (for example, nine-inch sequenced monitors), assessors should verify their function and sequencing (if employed). Check all PTZ functions for proper operation. Also check video recording systems.

Field-of-View Test
In conjunction with the perimeter intrusion-detection system test, assessors should conduct field-of view tests if the far point of the camera field of view appears to be excessively long (that is, a clear image of an intruder cannot be seen at the far end of the camera's field of view). To conduct this test, a person should be positioned at the far end of the field of view and should slowly walk across the isolation zone. This test should also verify that the inner perimeter fence line is within the field of view of each camera that observes the isolation zone.

Obstruction Test
A test should be conducted when an identified obstruction or shadow may preclude effective observation. This test is conducted by having a person run and hide behind the obstruction or in the shadowed area.

Speed of Response Test
At a narrow point in the isolation zone, a person should run through the intrusion-detection system sensor zone to the inner perimeter fence line. This test is used to verify that automatic camera call-up and/or video recording is sufficiently rapid to allow observation of the intruder before he can leave the isolation zone and the camera's field of view.

Test Guidelines:

- All of the foregoing tests should be conducted during daylight and at night to ensure that lighting is adequate and cameras can function properly in low-light conditions. Additionally, the functional test should be conducted at sunrise or sunset to verify that positioning the camera directly toward the sun doesn't degrade camera functions.

- At a minimum, testing of at least two camera zones should be conducted.

- Obstruction tests should be conducted whenever functional tests indicate that the assessment capability in a camera zone is significantly degraded by the obstruction.

- If a significant number of camera zones (more than 10 percent) exhibit degraded picture quality, maintenance records should be reviewed to determine whether useful camera life limits might have been reached due to not replacing camera image tubes.

INTERIOR CCTV TESTING

System Description: Fixed and PTZ cameras, wall or ceiling bracket-mounted; coaxial cable or fiber optic transmission; associated switching, display, and recording equipment.

Capabilities: Interior surveillance and intrusion assessment, with ability to differentiate between humans and animals, or other causes of false or nuisance alarms generated by the interior intrusion-detection system

Vulnerabilities: Inadequate lighting, improper alignment or overlap, and visual obstructions

Concerns:

- Cameras and associated supporting systems (switches, monitors, and recorders) are complex devices requiring extensive maintenance and calibration. Certain components (especially camera image tubes) are subject to predictable failure as they age. Failure because of aging may be a system-wide occurrence if several cameras were installed at the same time.

- Visual obstructions can block camera fields of view, creating the potential for intruders to hide or to cross the camera zone without being observed.

- Camera image tube and video monitor burn-in can result from constant focus on a high-contrast background (extreme light to dark ratio), which degrades camera and video monitor performance.

- If camera placement or alignment is improper, there may be "holes" in the CCTV coverage that could permit unobserved intruder access. Additionally, if the camera's field of view is too long for the camera lens, an intruder at the extreme end of the field of view may not be adequately observed.
  (Note: Industry requires the postulated adversary to occupy at least five vertical scan lines when standing at the far end of the camera's field of view.)

- Automatic camera call-up on the alarm monitor at the CAS/SAS upon activation of an intrusion detection system sensor (if employed) should be rapid enough (no more than two seconds) to observe the intruder before he/she crosses the camera's field of view. Alternatively, the video recording system (digital or laser disk) should be capable of recording and playing back the camera scene showing the intruder crossing the camera zone.

- PTZ cameras should have limit switches so they will not face directly into bright light sources. Also, if PTZ cameras are automatically called up by intrusion-detection system activation, they should be programmed to automatically position themselves to view the area from which the alarm was received.

Types of Tests:

Functional Test

A functional test of each camera should be performed from the CAS/SAS by calling up each camera scene to verify that all cameras are operating and that a clear image is received. If multiple monitors are used for continuous display, their function and sequencing (if employed) should be verified. Any PTZ functions should also be checked for proper operation, as should video-recording systems.

Field-of-View Test

In conjunction with the interior intrusion-detection system test, field-of-view testing should be conducted if the far point of the camera's field of view appears to be excessively long (that is, a discernible image of an intruder cannot be obtained at the far end of the camera's field of view). To conduct this test, a person should be positioned at the far end of the field of view and should walk slowly across that field of view. In general, this test should also verify that critical access portals are within the camera's field of view.

Obstruction Test

A test should be conducted whenever an obstruction and/or lighting conditions could preclude effective observation. This test is conducted by having a person hide behind the obstruction or in a darkened area.

Speed of Response Test

To test for speed of camera response when automatic call-up of a camera upon intrusion-detection system activation is employed, a person should activate an interior sensor and then attempt to rapidly exit the area covered by the camera. This test is used to verify that automatic camera call-up and/or video recording is rapid enough to allow observation before the intruder can leave the camera's field of view.

Test Guidelines:

- All the foregoing tests should be conducted under day, night, and overcast conditions to ensure that the cameras can function in all light conditions, as applicable.

- At a minimum, test at least two camera zones, if possible.

- Conduct obstruction tests whenever functional testing indicates that the assessment capability in a camera zone is significantly degraded by an obstruction.

- If a significant number of camera zones (more than ten percent) exhibit degraded picture quality, maintenance records should be reviewed to determine whether useful camera life limits have been exceeded because camera image tubes have not been replaced.

ALARM PROCESSING AND DISPLAY EQUIPMENT

General Characteristics: CAS/SAS alarm consoles, alarm annunciators and displays, system status indicators, CCTV monitors and recorders, personnel and vehicle access controls, lighting and emergency power controls, and various support equipment

Capabilities: Security system monitoring, control, assessment, and historical recording, as appropriate; redundant command and control capabilities at CAS and SAS

Vulnerabilities: Poor human-machine interface, excessive numbers or differing types of displays, inadequate redundancy between CAS and SAS

Concerns

- High numbers of nuisance/false alarms may degrade operator response to genuine alarm conditions.

- Failures of the system to adequately identify alarm type and specific location may degrade response. This is usually most evident in systems that do not clearly differentiate between tamper-indication or line-supervision alarms, or when multiple sensors are monitored by a single circuit (for example, alarms in series).

- In older systems, which do not use a computer-based integrated alarm processing system, a variety of different alarm panels and status indicators may be employed. This can cause inefficiency and confusion in assessing and acknowledging alarms because the operator must respond to several standalone annunciators.

- In older computer-based systems, problems may arise from the computer's lack of speed or from inadequate alarm prioritization. In those cases, the system is unable to expeditiously and effectively sort significant quantities of simultaneous, or near simultaneous, alarm information and the system becomes bogged down resulting in slower alarm processing, storing alarm information without prioritization, or (in the worst case) a system crash. If such conditions were to occur, the ability of the operator to provide timely detection/assessment information to the protective force would be severely degraded, as would the protective force's ability to rapidly respond.

- For computer-based systems, problems may also arise as new or additional sensors or access control devices are added over time. Each time the system configuration changes, software programming changes are required in the system. Unless software modifications and system configuration are carefully controlled, program errors may be generated.

Types of Tests

Function Test

Assessors should perform a functional test of each type of alarm annunciator, status indicator, or control device in conjunction with each subsystem test (for example, CCTV, intrusion-detection system, access control, emergency power test). The purpose of each test is to verify proper system function and to determine whether alarm annunciation, acknowledgement, and command/control are clear and straightforward. Promptness of alarm display following field device activation should be checked concurrently.

Historical Record Test

Evaluate any historical records maintained by the system (for example, alarm logs, access control transaction histories, and video recordings) for completeness and accuracy. False and nuisance alarm rates may also be assessed by reviewing these records.

SAS Test

Test a representative number of alarm annunciations and command/control functions at the SAS to determine that the SAS provides adequate backup to the CAS. As part of this testing, inspectors should verify that the SAS is capable of knowing about any command actions taken by the CAS that change alarm points or access control devices from the secure mode to the access mode or that enable/disable security devices.

Test Guidelines:

- Conduct testing of alarm processing and display in conjunction with other system tests.
- Test CCTV displays and recording capabilities during both daylight and darkness.
- At a minimum, test at least one of each type of alarm annunciation, recording device, and command/control function.
- Conduct a separate limited-scope performance test of the SAS to verify its adequacy as a backup to the CAS.

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/her 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 assessors 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 assessors 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.

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 involves observing a security technician as he/she 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

Assessors 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. Assessors 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 assessors might conduct testing of the SPO's visual search procedures involving a lead container in a toolbox.

Test Guidelines:

- Typically, the assessors 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 assessor`s 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 assessors should conduct testing to exploit those deficiencies in order to determine their significance/extent. For example, if the assessors note that a SNM walk-through detector is not adequately monitored by SPOs, then the assessors 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, assessors 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 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 more detectors. Rarely would an assessor 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.

DOCUMENT GENERATION TEST PERFORMANCE TEST

Objective: To determine whether personnel responsible for generating classified documents are doing so in accordance with DOE requirements.

Scenario: The team member selects a sample of personnel who normally generate classified documents. These personnel are asked to generate simulated classified documents and are observed to determine whether they follow required procedures for tracking, controlling, obtaining classification review, marking, and accounting for (as applicable) these documents.

DOCUMENT MARKING TEST PERFORMANCE TEST

Objective: To determine whether personnel responsible for marking classified documents are doing so in accordance with DOE requirements.

Scenario: To specifically verify the test participant's ability to mark classified documents, the team member gives the classified document handlers several simulated classified documents along with a complete description of the nature and contents of the documents, such as classification level, category, and authority. Each test participant is then asked to properly document and mark the documents.

Variation: Employ the same scenario as above, but substitute microfiche, viewgraphs, messages/cables, or other media for a typical paper document.

INTRASITE CROSS-CHECK PERFORMANCE TEST

Objective: To verify that documents sent within a site can be produced, or their disposition determined, at the receiving site organization.

Scenario: The team member uses an organization's document accountability records to identify classified documents that were recently transmitted to another organization within the same site. The team member then verifies that the receiving organization's accountability log reflects the receipt and that the organization can produce (1) the documents themselves, (2) their destruction forms, or (3) their transmittal slips.

CUSTODIAN RECEIPT PERFORMANCE TEST

Objective: To determine whether those receiving classified matter follow appropriate custodian receipt procedures.

Scenario: To verify appropriate custodian receipt procedures, a sample of document custodians who normally receive classified matter is selected for testing. Each test participant is sent a simulated Secret document through normal channels. The team member must then ascertain whether the recipient properly signs receipts for, checks, and enters the document into accountability.

Variations:
(1) Send to a test participant a simulated Secret document that was incorrectly transmitted, was incorrectly or incompletely marked, or is missing pages. Verify his/her response (e.g., to return the document, issue an infraction, or initiate other action).
(2) Prepare a classified document to be sent off site through the classified mail. The document prepared should indicate a classification level/category that the receiving facility is not authorized to accept. Verify

REPRODUCTION PERFORMANCE TEST

Objective: To determine whether classified documents are reproduced in accordance with DOE directives.

Scenario: The team member selects a sample of personnel for testing who normally reproduce classified documents. Test participants are asked to demonstrate their procedures for duplicating classified documents (genuine or simulated) to determine whether they comply with the requirements for using approved (and posted) locations/equipment, running the appropriate number of blanks after duplicating, treating those blanks as classified waste, controlling documents for reproduction if they are normally dropped off at a central reproduction station, and documenting/marking reproduced copies.

Variations:
(l) Use the same scenario but instead of a typical paper document, use microfiche, viewgraphs, blueprints, or any other type of medium containing classified information.
(2) Carry out the scenarios at the inspected site's print shop, photo lab, or other facility tasked with reproducing classified information.
(3) Submit improperly/incompletely marked simulated classified documents for reproduction and determine whether discrepancies are noted.

REPOSITORY CHECK PERFORMANCE TEST

Objective: To determine whether repositories used to store classified documents are being routinely checked, and to ascertain whether appropriate actions are taken if a repository is left unsecured.

Scenario: Team members visit selected locations in which classified matter is stored and/or used. Team members arrange with someone having access to a repository to leave it open (simulated by using a sign or by substituting authentic classified documents with simulated ones). Actions by those responsible for security-checking the repository are observed. [Note: Scenario requires safety plan and coordination with the protective force.]

DOCUMENT ACCOUNTABILITY PERFORMANCE TEST PLAN – FRONT CHECK

Objective: To evaluate the accuracy of the DOE San Diego Operations Office (SDO) document accountability system and to determine whether documents are protected, stored, and marked in accordance with DOE requirements.

System Description:
The document accountability is maintained using a manual system of document receipts. Document control "tickets" may reflect more than a single document. Tickets are filed in the SDO mail room, which also provides centralized dispatch and control. Individual custodians also maintain records of their holdings. Although individual custodians may have entered holdings in their personal computers, no computer enumeration of a master list of active holdings or system-generation of random samples is possible.

Sampling Technique:
SDO is unable to provide the total number of documents contained in active holdings. They estimate 2,400 control tickets are in use to reflect active holdings, but some tickets represent multiple copies of documents.

The Office of Independent Oversight (OIO) will select a random sample of 200 documents by computer

generating a list of random numbers reflecting document control tickets. Corresponding control tickets will then be examined and documents reflected on the selected tickets will be used as the inspection sample for the front check of the DOE SDO accountability system.

Scenario:
Selected documents will be reviewed at their storage locations, or at a central location as appropriate. Each will be checked to ensure it is the item described in the accountability records. Additionally, documentation, markings, dates, titles, and pages will be checked to determine compliance with DOE requirements. Each repository will also be inspected for compliance with DOE storage requirements.

Safety Plan
Not required.

CLASSIFIED TRANSMITTAL PERFORMANCE TEST PLAN

Objective: This test is conducted to determine whether classified matter is transferred to and from the USPS, in accordance with requirements.

Scenario: Transfer procedures will be reviewed by tracking certified and registered mail from its receipt at the U.S. Post Office until it reaches its final custodian. Observation will include receipt from USPS personnel; transportation; delivery; entry into the appropriate accountability system; and custodian receipt procedures, as applicable.

Safety Plan
Not required.

CLASSIFIED DOCUMENT DESTRUCTION PERFORMANCE TEST PLAN

Objective: To determine whether classified documents are destroyed in accordance with DOE directives.

Scenario: Team members will observe personnel destroying classified matter, using routine local procedures. Should destruction of classified not be planned during the assessment, site personnel will be asked to describe procedures or perform actions on simulated classified matter.

Safety Plan
Not required.

DATA COLLECTION SHEET: PREVIOUSLY IDENTIFIED DEFICIENCIES

CLASSIFICATION

CLASSIFIED MATTER PROTECTION AND CONTROL

PREVIOUSLY IDENTIFIED DEFICIENCIES

Deficiency	Date Identified	Discovered by	Corrective Action	Est. Completion date	Validated by

CLASSIFICATION

PERSONNEL SECURITY: SAFEGUARDS AND SECURITY AWARENESS PROGRAM

Objective: To determine the effectiveness of the facility's S&S Awareness Program.

Scenario: Review the security education briefings (initial, comprehensive, and refresher). Select a number of employees who have attended the various briefings. The assessment team member will interview these employees with the same questions for the type of briefing they received. (The questions and associated correct answers will be prepared during assessment activities as they will be site-specific.) The assessment team member will complete an evaluation form for each interview (to be prepared during the assessment).

Evaluation Criteria: 90% of the interview questions must be answered correctly.

MATERIAL CONTROL & ACCOUNTABILITY- DOCUMENT SAMPLING

Objective: This test will determine whether the accounting system is in compliance with all reporting requirements.

Scenario: Randomly select a sample of accounting documents to verify accuracy and completeness and then use this sample to physically locate material. (May be used with the tests for accountability, data traceability, and item location.)

Evaluation Criteria:

a. Were all records complete, accurate, and submitted in a timely manner?
b. If discrepancies exist, are they a systemic problem or isolated cases?
c. Does the information in the records agree with the physical inventory?

VULNERABILITY ASSESSMENT (VA) VALIDATION CHECKS

Objective: Determine whether the detection probabilities used by the facility are supported in the VA.

Scenario: Review the VA and select several detection probabilities. Ask the facility to produce the documentation that supports the detection probability.

Evaluation Criteria:
a. Does documentation exist to support the VA detection probability?
b. Does performance testing data support the detection probability that was assigned?
c. Does the facility have an ongoing performance testing program to support the detection probability?

MATERIAL CONTROL & ACCOUNTABILITY
INTERNAL REVIEW AND ASSESSMENT PROGRAM OBSERVATIONS

Objective: Determine whether the facility can perform an internal review by observing an actual assessment.

Scenario: Select an internal review topic and an area to be reviewed. Ask the facility to conduct an internal review. Observe the review, or introduce an anomaly by having a finding (using the individual to be reviewed as a trusted agent) to determine whether the internal review is effective in detecting that finding.

Evaluation Criteria:
a. Is the reviewer knowledgeable in the area being reviewed?

b. Is the topic being reviewed documented in the internal review and assessment program plan?

c. Are communications between the reviewer and reviewee clear and concise?

d. If there were any findings, did the reviewer effectively communicate them to the reviewee?

e. If an anomaly was introduced by the inspector, was it detected?

f. Were appropriate actions taken?

MATERIAL CONTROL & ACCOUNTABILITY
ACCOUNTING SYSTEM

Objective: This test will determine whether the materials accounting system can function following system failures at different levels and whether the system can be recovered.

Scenario: Simulate failure of different levels of the accounting system, including online data entry points on process lines or sensors, primary accountability computers, and primary storage media.

Evaluation Criteria:
a. Were operations successfully restarted?

b. Was there resolution of all items, operations, and measurements affected while the system was down?

c. Was the system successfully restarted from backup data or systems?

MATERIAL CONTROL & ACCOUNTABILITY
CLOSURE OF CORRECTIVE ACTIVE VALIDATION

Objective: Determine whether closed findings from the internal review and assessment program have been appropriately closed.

Scenario: From a list of closed findings from the internal review and assessment program, select several closed findings. Validate the closed findings through field inspections.

Evaluation Criteria:
a. Were the findings stated as closed by the facility still closed?

b. Were the findings appropriate for the identified deficiency?

c. Were the closure actions still in place?

d. Did the corrective action address the root cause of the deficiency?

MATERIAL CONTROL & ACCOUNTABILITY
MATERIAL TRANSFER CHECKS FOR MBA CATEGORIZATION

Objective: This test will validate the facility controls to ensure that a Category II or III MBA cannot receive material that would increase the category level.

Scenario: Attempt a material transfer (using only documentation not actual material) to a Category II or III MBA to increase the category of the MBA.

Evaluation Criteria:
a. Do procedures exist to prohibit the increase in category level for MBAs?

b. Was the attempted transfer detected?

c. Was the facility response to the attempted transfer appropriate?

MATERIAL CONTROL & ACCOUNTABILITY
MATERIAL ACCOUNTING: ITEM IDENTIFICATION FRONT AND BACK CHECKS

Objective: This test will determine whether the facility records accurately reflect the identity, value, and location of inventory items.

Scenario: Select a sample of items from either the inventory listing or during the field inspections. Record the item ID, location, plutonium weight, and tamper indicating device (TID). Verify the items in the field or the sample taken from the field to the accountability system records.

Evaluation Criteria: Were items in the field successfully reconciled to the nuclear material accounting system records?

MATERIAL CONTROL & ACCOUNTABILITY
SNM RECEIPT CLOSURE

Objective: Determine whether transactions (receipts) with unmeasured values or significant shipper/receiver differences are entered into the process.

Scenario: Utilize a TJ-14, "Transaction Activity Summary By Facility," generated by the Nuclear Material Management and Safeguards System (NMMSS) to test facility records.

Evaluation Criteria
a. Are receipts measured and transactions closed prior to introducing material to process?

b. Are exceptions granted for those materials that do not have a measurement or for transactions not completed?

MATERIAL CONTROL & ACCOUNTABILITY
MATERIAL ACCOUNTING: ACCOUNTING SYSTEM FORMS

Objective: This test will determine the effectiveness of the system utilized for filing controlled accountability forms used in the Material Balance Area (MBA). Check key information on documents reviewed, including form used for transfers of special nuclear material (SNM).

Scenario: For each type of control and accountability record, randomly select 10% (or a minimum of 1) of the forms used in the MBA during the review period. Locate these specific records and check key entries for completeness.

Evaluation Criteria:
1. Could all forms be located during the field investigation portion of the review?

2. Were all corrections or lineouts initialed by the custodian done in accordance with requirements?

3. Did all of the forms contain the required information?

MATERIAL CONTROL & ACCOUNTABILITY
MATERIAL CONTROL: TAMPER INDICATING DEVICE (TID) SYSTEM

Test Objective: This test will determine whether TID discrepancies are detected and if proper resolution is achieved.

Scenario: Replace a TID with another TID without initiating changes in accounting records; OR make a change in the TID number in the accounting records.

Evaluation Criteria:
1. Was the different number detected?

2. Were records checked to verify which TID should be on the item?

3. Was the item remeasured to verify the special nuclear material (SNM) content?

MATERIAL CONTROL & ACCOUNTABILITY
MATERIAL CONTROL: MATERIAL SURVEILLANCE – TWO-PERSON RULE

Test Objective: This test will determine if the two-person rule can be compromised.

Scenario: One person of the two-person rule requests that the other person leave to get additional supplies. The scenario can be tested in vaults, processing areas, waste assay and packaging areas, Tamper Indicating Device (TID) applications, etc.

Evaluation Criteria:
1. Did the person leave the area?

2. Was a second authorized person called to provide two-person coverage?

MATERIAL CONTROL & ACCOUNTABILITY
MATERIAL ACCOUNTING: MEASUREMENTS AND MEASUREMENTS CONTROL – SCALES AND BALANCES

Objective: This test will determine whether the Scales and Balances program provides data of the quality required for MC&A records.

Scenario: Select a sample of accountability weighing instruments from the MC&A organization records and verify the frequency and currency of the calibration and the performance of daily linearity checks. Check the performance of the instrument against standards normally used or against independent weight standards that are in the normal weighing range of the instrument.

Evaluation Criteria:
1. Was instrument calibration current?

2. Are appropriate standards being used?

3. Are daily checks being made?

4. Were personnel familiar with the operation and MC&A procedures?

5. Did the instruments perform to the stated specification?

MATERIAL CONTROL & ACCOUNTABILITY
SNM ITEM LISTING GENERATION

Objective: Determine whether the facility can generate a physical inventory listing for MBAs possessing Category I SNM within 3 hours, or within 24 hours for other MBAs.

Scenario: Ask the facility to generate an inventory listing and note how long it takes to generate the listing. (This scenario can be combined with an actual physical inventory. The inspector can introduce an anomaly into the inventory list and evaluate the facility response.)

Evaluation Criteria
1. Was the inventory list generated within the appropriate timeframe?

2. Was the list accurate?

3. How did the facility consider items in transit or data that had not been entered into the computer system?

4. If an anomaly was introduced, did the facility detect it and initiate appropriate action?

MATERIAL CONTROL & ACCOUNTABILITY
INTERNAL TRANSFER FORMS FALSIFIED

Objective: Determine whether the facility can detect a falsified internal transfer.

Scenario: A facility transfer form is prepared by an unauthorized individual and processed through the accountability system.

Evaluation Criteria:
1. Did the facility procedure for processing transfers detect the falsified transfer?

2. Was the facility response appropriate and timely?

FOREIGN VISITS AND ASSIGNMENTS (FNVA) PROGRAM
SPONSOR PROGRAM MANAGEMENT AND ADMINISTRATION

Objective: This test will be used to determine that a system/process is implemented to ensure DOE requirements are met regarding a visit by a foreign national from a non-sensitive country.

Scenario:

a. The assessment team member will prepare a request for an unclassified visit to the facility by a foreign national from a non-sensitive country.

b. The assessment team member will review the facility procedures for implementation and then coordinate with a facility representative to submit the request to the visitor control staff.

c. The assessment team member will observe the visitor control staff in the processing of the visit request from start to finish, noting if correct forms and plans are used.

Conditions: Normal work conditions.

Evaluation Criteria: Facility implementation procedures are followed.