

OVERSIGHT

Context and Protocols for Performance Testing of Protective Forces

February 1999



Office of Environment,
Safety and Health



TABLE OF CONTENTS

1.0	Purpose	1
2.0	Background	1
3.0	Definitions	2
4.0	General Planning and Conduct Guidelines	4
5.0	Responsibilities for Test Planning and Conduct	6
5.1	Personnel	6
5.2	Planning	7
5.3	Scenario Development	8
5.4	Test Conduct and Control	8
5.5	Evaluation	8
5.6	Logistics	8
6.0	Adversary Team Role and Guidelines	9
6.1	Adversary Team Role	9
6.2	Scenario Planning Responsibilities	10
6.3	Intelligence Gathering and Reconnaissance	10
7.0	Design Basis Threat and Adversary Team Capabilities	11
8.0	Participant Selection	11
9.0	Safety	12
10.0	References	12

Appendix A: Adversary Team Capabilities Inventory
(Published separately)

OVERSIGHT

1.0

Purpose

This document describes the context and protocols associated with that portion of the Office of Security Evaluations' oversight program dealing with the performance testing of protective forces. It sets forth basic guidelines, procedures, and responsibilities for planning, conducting, and evaluating protective force performance tests that are part of the Office of Security Evaluations' formal oversight activities. Although it describes Security Evaluations' overall approach and basic requirements for implementing its performance testing philosophy, this document does not provide or prescribe detailed procedures for performance test planning or conduct.

There are recognized differences among the various protective forces, physical facilities, and security interests within the DOE community; these differences require a flexible approach to the application of testing and evaluation techniques. While this document describes common guidelines and procedures applicable to most performance testing Security Evaluations will require, it does not restrict the types of performance tests Security Evaluations may conduct or the manner in which they are conducted. Within the general testing philosophy expressed in this document, Security Evaluations will conduct the types of performance tests it deems necessary, using the procedures it deems necessary and appropriate, to accomplish its oversight mission.

This document supersedes the Office of Security Evaluations' May 1990 *Guidelines and Procedures for OSE Protective Force Performance Tests*.

2.0

Background

Performance tests have been an important part of Security Evaluations' and its predecessor organizations' activities since the inception of formal oversight of safeguards and security in the Department of Energy (DOE). Performance testing continues to play a significant role in Security Evaluations' oversight activities. The most appropriate and useful method of evaluating a protective force's ability to perform certain routine and emergency duties in its operating environment is to observe it performing those or similar duties under controlled, and sometimes simulated, conditions—that is, in performance tests. Security Evaluations' performance tests range in complexity from simple demonstrations of a single individual skill to major integrated tests involving an entire protective force shift operating with other elements of a facility's security system.

Historically, artificialities driven largely by operational limitations and safety concerns have influenced and often constrained performance testing activities—particularly large scale, complex tests and those involving firearms and force-on-force action. In recent years requirements spurred by increased safety concerns have resulted in more formal, prolonged, and detailed planning and more stringent guidelines for conducting performance tests that involve firearms of any kind. Consequently, the appropriate site organizations must now play a much larger part in planning and conducting performance tests associated with oversight activities. Notwithstanding the larger role of site organizations, performance tests conducted for Security Evaluations oversight purposes must be planned, conducted, and evaluated in accordance with the protocols established herein and in a manner that promotes achievement of appropriate oversight goals.

Adversary Team. Players who act in the roles (as indicated by the prescribed scenario) of adversaries during performance tests. May be composed of Composite Adversary Team (defined below) members or personnel from other sources. May also include Insiders (defined below).

Composite Adversary Team. A designated team of DOE Security Police Officers drawn from throughout the DOE complex to support Security Evaluations performance tests by acting as members of the adversary team.

Controller. An individual assigned responsibilities to assist in the control of a performance test. Such responsibilities generally include enforcing rules of conduct, safety rules, and other control measures, as well as ensuring the timely and proper accomplishment of specific scenario events. Controllers are normally trained and certified to perform their duties, and are normally provided by organizations at the inspected site and its responsible DOE operations office. Under appropriate circumstances, Security Evaluations Evaluators may also perform Controller duties.

Engagement Simulation System (ESS). Equipment consisting of weapons-mounted laser transmitters and laser sensors mounted on potential targets (e.g., personnel, vehicles, buildings). ESS permits accurate assessment of weapons effects during simulated hostile engagements. Synonymous with MILES (defined below).

Evaluator. An individual who is assigned responsibility for formally evaluating the performance of security system elements during a performance test. For oversight activities, Security Evaluations provides the Evaluators from its pool of personnel who have been trained and certified as Controller/Evaluators.

Insider. A person from the inspected facility who is assigned to assist the Adversary Team to the best of his/her ability. For purposes of a performance test, an insider is considered to be part of the Adversary Team. Insiders may be either active or passive, depending upon DOE threat guidance, the Site Safeguards and Security Plan, the position occupied by the Insider, and the details of the scenario being tested.

The normal definitions of active and passive Insiders, as applied to Security Evaluations performance tests, are:

- **Active Insiders** directly participate in actions of the Adversary Team or actions in support of the Adversary Team and its goals. They have the same level of motivation as the rest of the Adversary Team. Depending upon their role, they may be armed and may be willing to kill and/or be killed.
- **Passive Insiders** assist the Adversary Team by participating in a covert manner. Some examples of passive insider actions include obtaining and/or supplying information, deliberately failing to report Adversary Team actions, opening or unlocking doors, and triggering alarms. Passive Insider actions would generally carry little risk of discovery during their commission. Passive insiders are not willing to kill or risk being killed.

Limited Scope Performance Test (LSPT). A performance test designed to evaluate specific skills, equipment, or procedures. The events of an LSPT may be interrupted to facilitate data gathering, and the events may be directed or redirected by Security Evaluations personnel in order to achieve certain evaluation goals. Although used as a data collection method for input to

various rated topics, LSPTs are not themselves rated. An LSPT may or may not involve the use of: ESS/MILES; live fire; and/or role players or an adversary team.

Major Performance Test. A large scale performance test that is usually enhanced by the use of ESS/MILES and is designed to test the ability of protective force skills, procedures, and equipment to deal with a scenario threatening a DOE security interest. A major performance test may also evaluate other aspects of a security system (e.g., alarm systems, barriers, etc). Major performance tests always employ an Adversary Team. Although each test includes a planned scenario, major performance tests involve considerable free play. The data collected during major performance tests is used as input for various rated topic areas, but the performance tests themselves are not individually rated.

Multiple Integrated Laser Engagement System (MILES). Equipment consisting of weapons-mounted laser transmitters and laser sensors mounted on potential targets (e.g., personnel, vehicles, buildings). MILES permits accurate assessment weapons effects during simulated hostile engagements. Synonymous with ESS (defined above).

Observer. An individual who observes a performance test, but who is not a Player and has no responsibilities for controlling the test or evaluating Player performance.

Performance Test Window (also Exercise Window). The portion(s) of the performance test process when scenario activities may be executed and elements of the protection system are being evaluated. The window is normally opened when all Players, Controllers, and other participants are in place and ready to begin and all administrative, logistical, and safety requirements for testing have been met. The window is normally closed when test objectives have been met, further useful scenario activity is unlikely, or some other event requires test termination. All evaluated scenario activity takes place during the performance test window, and no activities taking place before or after the window are considered part of actual performance test (scenario) play. When multiple scenarios or multiple iterations of a scenario are conducted, each scenario or iteration has a distinct

window. Performance test windows are normally used only for tests employing force-on-force types of activities.

Player. An active participant in a performance test. May be a member of the site protective force, other Federal agencies, local law enforcement agencies, (role-playing) site employees, or the Adversary Team.

Safety Coordinator (also Safety Controller, Safety Officer). An individual responsible for ensuring that performance test plans satisfactorily address safety-related DOE policy issues and site-specific safety concerns. Responsible for identifying and mitigating hazards associated with the performance test area and planned scenario/test activities so that the test can be conducted with realism and a reasonable level of risk. Safety Coordinators are assigned by Security Evaluations, the responsible DOE field element, and the facility contractor safety organization, as necessary. Safety Coordinators are Trusted Agents (defined below) and are subject to confidentiality requirements.

Senior Controller. An individual, responsible to the Test Director, who controls performance test preparations and conduct, and to whom all Controllers report. Normally provided by a facility contractor organization, usually the security or protective force organization. Security Evaluations designates a co-Senior Controller (usually a support contractor specialist) to work with the site's Senior Controller to ensure that appropriate test objectives are met.

Test Director. An individual who is assigned overall authority and responsibility for planning and conducting a performance test. Normally provided by a facility contractor organization, usually the security or protective force organization. Security Evaluations designates a co-Test Director (senior Federal staff member) to work with the site's Test Director to assist in achieving a realistic, safe, and valid test.

Trusted Agent. In general, neutral individuals whose involvement in the planning, coordination, or conduct of a performance test results in knowledge about test or scenario events that must be kept confidential in the interests of test validity. Primary Trusted Agents are usually assigned by the site protective force contractor (and the

responsible DOE field office, if appropriate) to assist Security Evaluations in developing, validating, and implementing scenario events and other test parameters necessary to achieve test objectives. The primary Trusted Agent(s) must have the authority to approve scenario events and test parameters on behalf of their organizations. Other

individuals involved in test planning, coordination, or approval—such as test planners, safety coordinators, and building managers—and who thereby gain some level of knowledge regarding a test are also considered Trusted Agents and are expected to keep all test-related information confidential.

4.0

General Planning and Conduct Guidelines

Security Evaluations uses performance testing to collect data on the capabilities of site protective forces and other security system elements as they relate to the protection of DOE security interests. To develop useful and valid information, the controlled conditions under which performance tests are conducted must be as realistic as possible, and any necessary constraints and artificialities must be designed to have as neutral an effect on player performance as possible. To meet the objectives of the oversight process, Security Evaluations has established the following general guidelines for performance testing conducted for oversight purposes:

- Security Evaluations does not draw win-lose conclusions from the outcome of any single performance test, including a major performance test. Performance tests are used to evaluate various skills, procedures, equipment, strategies, and tactics, and to identify trends. The insights gained from performance tests are factored into overall conclusions about the protection system or elements thereof.
- Security Evaluations performance tests are usually not rated and are never based on win-lose criteria.
- Security Evaluations will accept a facility's established performance testing

procedures (planning protocols, rules of conduct, safety rules, etc.) as long as they are deemed to be reasonable, fair, and supportive of Security Evaluations' performance testing objectives. Any local practices that do not meet oversight needs will be amended based on discussion and agreement between Security Evaluations and the appropriate Trusted Agent(s).

- Security Evaluations will determine what to test and will determine certain scenario events. For example, Security Evaluations may want to test the effects of certain adversary weapons or tactics, or tailor scenario events to complement or validate information derived from tabletop exercises or Joint Tactical Simulation System runs. Within the parameters provided by Security Evaluations planners, the adversary team will be allowed to develop specific details of their plan for mission accomplishment, subject to the approval of Security Evaluations and the agreement of the primary Trusted Agent(s).
- Security Evaluations will make the final decision regarding whether a planned performance test has a reasonable chance of achieving oversight goals. If Security Evaluations determines that the artificialities and/or restrictions associated

with a planned test are so severe as to jeopardize the realization of valid results, Security Evaluations may determine, at its discretion, not to conduct the test.

- Security Evaluations will not recognize or be bound by artificial limitations or unreasonably narrow interpretations of Design Basis Threat capabilities. (See Section 7 for a discussion of the applicability of the Design Basis Threat and adversary capabilities.)
- All Trusted Agents and other personnel involved in test planning and/or conduct must strictly maintain the confidentiality of scenario and other test-related information.
- To the extent possible, performance test plans, procedures, control measures, and simulations must be designed to achieve maximum realism in test play, an overall neutral effect on player performance, and an acceptable level of risk to all participants.
- Performance testing activities should be conducted as safely as possible while accommodating the need to achieve an acceptable level of realism.
- To the extent reasonably possible, adverse impacts of performance tests on site operations should be minimized. This can often be accomplished through early planning and cooperative scheduling.
- Security Evaluations personnel will evaluate the performance of security elements being tested, and will draw appropriate conclusions from their evaluation effort. Organizations being evaluated may concurrently have their own personnel (e.g., Controllers) independently evaluate the performance of security elements, if such an evaluation would further their own organizational goals.
- To better accommodate the identification of trends, multiple tests or multiple iterations of tests will be conducted whenever possible. It

is preferable that a series of tests involve as many different protective force shifts (and personnel) as possible.

- Artificialities associated with test play should be minimized. Simulations are generally a poor substitute for actual performance and should be used only when unavoidable.
- Performance testing should be conducted on the terrain and in the facilities and buildings where an actual battle (to protect the security interest targeted by the scenario) would be fought. Use of alternate or mock facilities does not normally provide an adequate indication of protective force performance in their actual operating environment.
- Restrictive control measures, such as test area boundaries and off-limits areas, should be based primarily on the needs of scenario play and should constrain the free movement of players as little as possible. While the needs of test control, participant safety, and operational convenience must be considered, artificial or unnecessary levels of restriction should be avoided.
- Simulations, when necessary, should be as realistic as possible. Simulations constructed to represent adversary actions that cannot be allowed (e.g., parachute insertion, helicopter insertion, explosive breaching of barriers) should not result in a disadvantage to the adversary team that would not result from their performance of the actual act being simulated. Security Evaluations representatives and the primary Trusted Agent(s) will develop reasonable and acceptable simulations when required.
- At all times when the performance test window is open, the players (including the site protective force) must maintain a “normal” posture for the conditions being simulated. “Normal” posture, as identified by previous observation of personnel on duty, must be enforced by test Controllers. Normal posture includes appropriate participants. Normal shift personnel

must stand their normal posts; in particular, other personnel who might be thought to perform better cannot be substituted for test purposes.

- The adversary team is not being tested or evaluated. While they will be required to accomplish realistic actions (e.g., carry needed equipment or simulated equipment, place simulated explosives, perform necessary movements/maneuvers, engage the protective

force), they will not be required to accomplish actions that are largely irrelevant to test objectives or to demonstrate skills that must be simulated for safety or other reasons. For example, they will not be required to travel long distances over land to reach the point of first detection, and they will not have to demonstrate expertise in use of explosives or other specialized equipment or in precision parachuting, even though the scenario may call for such skills.

5.0

Responsibilities for Test Planning and Conduct

Most facilities and protective force organizations now have specific, approved local procedures for performance tests or exercises involving the use of ESS/MILES equipment. It is common for the planning, coordination, and approval process for performance tests to commence up to several months before a test date and involve many formal steps and milestones. Whenever possible, Security Evaluations will observe these local requirements.

The time on site and familiarity with site facilities, procedures, and personnel required to plan a major performance test while observing local requirements make it impractical for Security Evaluations personnel to play the primary role in detailed planning and test control. Major responsibility for detailed test planning and conduct therefore falls to the inspected site. Performance testing associated with oversight activities is a cooperative effort of Security Evaluations and the inspected facility, in which Security Evaluations establishes expectations and participates in the planning process, the appropriate site organization(s) accomplish detailed planning and test conduct, and Security Evaluations provides specific logistical and control support and evaluates performance. Major responsibilities regarding personnel, planning, scenario development, test conduct and control, evaluation, and logistics are described below.

5.1 Personnel

Security Evaluations will provide the following personnel:

- A co-Test Director to work with the site Test Director to ensure that test plans and conduct meet Security Evaluations' needs.
- A co-Senior Controller to work with the site Senior Controller to ensure that the planning details and conduct procedures are mutually agreeable and supportive of performance test goals.
- A safety representative to work with the site Safety Controller (coordinator, officer) to ensure that test planning and conduct address identified hazards and other safety issues.
- Evaluators to assess performance during the test. Evaluators are trained and certified as Controllers by Security Evaluations and can also perform Controller functions if necessary, as long as those functions do not impede the performance of their evaluation responsibilities.

- The adversary team, which will play the part of the adversaries during the performance test.

The inspected facility will be expected to provide the following personnel:

- A Test Director to oversee the planning and conduct of the performance test.
- A Senior Controller to control the conduct of the performance test. Depending upon site procedures, the Senior Controller may also be responsible for supervising detailed test planning.
- A primary Trusted Agent to work with Security Evaluations in agreeing upon scenario events, simulations, and other details of test conduct. Often the primary Trusted Agent is also the Test Director or Senior Controller.
- Limited Trusted Agents, if necessary to accomplish planning and coordination details (e.g., facility managers, safety officer).
- A Safety Coordinator (Controller, Officer) responsible for identifying and mitigating potential hazards and monitoring test planning and conduct to ensure that accepted reasonable risk levels are not exceeded.
- Planners to work out the administrative, logistical, and operational aspects of the test and to develop the performance test plan.
- Controllers to perform assigned duties under the direction of the Senior Controller to ensure that the test is conducted safely and according to approved plans.
- Protective force personnel to be tested.
- An Insider (if necessary) to participate as a part of the adversary team during planning and, if appropriate, during test conduct. (Note: A different Insider may be required for each

scenario, particularly if the scenarios involve different facilities.)

- Role players (if necessary) to play the parts of workers or any “players” in the test other than the protective force and adversary team players.
- Any site personnel who must be present or standing by during performance tests to comply with site requirements or agreements (e.g., shadow force, building managers, fire department, ambulance crew).

5.2 Planning

Security Evaluations will have the following planning responsibilities:

- To provide the site with overall performance test goals, objectives, parameters, and expectations in sufficient detail to allow the site planners to meet expectations.
- To select the target and develop the scenario. (Scenario details will be coordinated with the primary Trusted Agent.)
- To monitor the test planning process, providing any additional information, clarifications, and decisions needed by test planners.
- To determine the necessary placement of Evaluators during test conduct and coordinate their placement with the primary Trusted Agent and/or other appropriate facility test planners.

The inspected facility will have the following planning responsibilities:

- To accomplish the detailed planning and coordination necessary to conduct the performance test, including the publication of a Performance Test Plan (including Safety Plan /Safety Annex) to the level of detail and in the format prescribed by local performance testing procedures.

5.3 Scenario Development

Security Evaluations, including the adversary team, will have primary responsibility for developing the adversary attack scenario, including target selection and specific adversary actions. Security Evaluations will coordinate scenario development and scenario events with the site primary Trusted Agent(s).

The inspected facility is expected to assist in scenario development by:

- Providing Security Evaluations representatives (not adversary team members) with timely access to the facilities and information they need to determine appropriate targets, testing requirements, and scenario components.
- Providing primary Trusted Agent(s) who can represent the facility in assuring the reasonableness of proposed scenario events and in developing and implementing control measures and simulations (when necessary) associated with scenario events.
- Providing an Insider (when requested) to assist the adversary team in developing its plans. If an actual Insider is not deemed necessary, the facility will provide—normally through the primary Trusted Agent(s)—appropriate information that an Insider, if used, would be able to provide.
- Providing any information requested, including maps, building floor plans, and other site- and/or operations-specific information.

5.4 Test Conduct and Control

Security Evaluations will have the following responsibilities during performance test conduct:

- Security Evaluations' co-Test Director, co-Senior Controller, and Safety Coordinator will work closely with their facility counterparts (facility Test Director, Senior Controller, and Safety Coordinator) and assist them in any way necessary to assure the success and safety of the performance test.

- Ensure that Evaluators are prepared for their tasks and attend the required pre-test briefings.
- Ensure that the adversary team carries out the scenario events and fulfills its other responsibilities according to the approved test plan.
- When necessary and the subject of prior coordination/agreement with the facility, have Evaluators also perform Controller duties.

The inspected facility will have the following test conduct responsibilities:

- Conduct all required safety and other test-related briefings.
- Execute and control performance test preparations and conduct in accordance with approved procedures and the approved test plan; this includes all administrative, logistical, operational, security, and safety aspects of test activities.

5.5 Evaluation

Security Evaluations will prepare and provide certified Evaluators to observe and formally evaluate the performance of the elements of the site's security system being tested. Security Evaluations will determine the number of Evaluators to be used, their physical locations during the test, and the evaluation criteria to be used.

The inspected facility may—at its discretion and for internal purposes—concurrently collect its own evaluation data (normally using facility-supplied Controllers as Evaluators) independent of Security Evaluations' Evaluators.

5.6 Logistics

Security Evaluations will have the following logistics responsibilities:

- Arrange for (through the DOE loaner package administered by Allied Signal) the necessary ESS/MILES equipment (and associated

weapons), ammunition, smoke, and pyrotechnics necessary to equip all performance test players in accordance with test plans. ESS/MILES equipment will normally be the new generation of equipment that records, stores, and provides a readout of engagement details.

- Arrange for and/or provide specialized equipment needed by the adversary team.
- Arrange for and/or provide specialized equipment needed by Security Evaluations' Evaluators. This may include radios if the inspected facility cannot provide Evaluators with sufficient radios on the performance test Control Net.

The inspected facility will be responsible for providing all test-related logistical support except that provided by Security Evaluations (see above). Logistics requirements are normally similar to those associated with internal site performance tests, including but not limited to:

- All equipment, vehicles, and administrative transportation required for protective force participation in the performance test.
- All equipment (radios, etc) and transportation required by Controllers.
- The provision of emergency services (fire, medical, maintenance) as required by local procedures and/or the approved test plan.
- The provision of food/drink to test participants, if required.
- If available, Control Net radios for Security Evaluations Evaluators.
- If available, protective force (net) radios for selected Security Evaluations Evaluators.
- Planning/training facilities for adversary team use before and after the performance test.
- If necessary, vehicles for adversary team use during test play and/or for pre-test preparations.

6.0

Adversary Team Role and Guidelines

6.1 Adversary Team Role

The role of the adversary team is to play the part of whatever adversary is postulated for a specific test. Adversary types may run the full gamut of the DOE Design Basis Threat and could range from a disgruntled employee to a highly trained, well equipped, state sponsored terrorist organization. The adversary team is used to simulate, as closely as possible (within the constraints imposed by available time and equipment, safety considerations, and available skills), the actions of the postulated adversary. Individual members of the adversary team—or the team in aggregate—are not required to possess all of the skills or knowledge that the adversary

they are representing (e.g., terrorist cell) might possess. The adversary team is not being tested during Security Evaluations performance testing activities, and members of the adversary team are not required to personally demonstrate some of the skills (e.g., explosives, electronic systems, pilot, parachutist, etc.) attributed to the role(s) they are playing. However, to achieve as much realism as possible during testing, the adversary team will be required to physically perform or simulate the actions associated with a specific scenario (for example, explosive breaching operations). Within the control and safety parameters established for the test, the adversary team will actually perform the normal physical and tactical

activities (such as movement, communication, employment of smoke and simulated small arms, grenades, and mines) required to accomplish their assigned mission.

6.2 Scenario Planning Responsibilities

The adversary team will be assigned a target and a mission by Security Evaluations test planners. They may also be provided specific instructions regarding such things as methods and tactics, weapons, or equipment they are to employ, when such specific instructions are important to test objectives. Within the bounds of such guidelines, the adversary team is free to develop specific plans to accomplish their mission. These plans are subject to approval by Security Evaluations planners (co-Test Director, co-Senior Controller) in cooperation with the facility primary Trusted Agent(s). (“Approval” review, which is an informal process, considers safety, realism, fairness, and “do-ability” from a test control standpoint.)

When the facility has provided a person to play the role of an Insider, that Insider will be considered a part of the adversary team and will fully participate in the team’s information gathering and planning process.

6.2 Intelligence Gathering and Reconnaissance

The scope of information potentially available to adversaries, as characterized by DOE’s generic threat guidance, is practically unlimited because of the capabilities of modern intelligence-gathering equipment and techniques and the long timelines often available for collection. However, due to time and resource constraints, the adversary team has very limited opportunities to develop information for planning and conducting its missions. Consequently, the following guidelines will be followed regarding information that is provided to the adversary team and that the adversary team is allowed to collect.

The adversary team will be provided with any unclassified information they wish, including information concerning the facility, target, and site operations. The adversary team will normally be provided with classified information only if the scenario involves Insider assistance or if a pathway to specific classified information has been identified. Data deemed to be classified, but available through unclassified routes, will also be available to the adversary team. If an individual is provided to play the part of an Insider, that individual will normally provide classified information known to him or her or reasonably obtainable by him or her. If an Insider is postulated but is not provided, classified information will be provided to the adversary team but will be limited to information that the specific type of insider would have or could obtain.

In certain cases, particularly when no actual insider is provided, a member of the adversary team may be provided an unrestricted tour of the performance test area (including security areas, buildings, target areas, etc.) to partially compensate for terrain information that could be developed over time or with the assistance of an insider.

During the planning phase, adversary team members may observe the performance test area from areas generally accessible to the public and from controlled areas that can be accessed without significant chance of detection. Such observations will be conducted overtly so as not to raise alarm if detected. Such observations will be coordinated as necessary through the primary Trusted Agent(s), and any appropriate notifications will be made so as to avoid the possibility of a security incident should any of the team members be observed and reported.

NOTE: If members of the adversary team are detected while engaged in pre-test activities, such as conducting surveillance or validating aspects of the planned scenario, such detection will not affect the protective force posture during the performance test. In addition, observation of authorized adversary team movements prior to the opening of the performance test window will not be used to alert or reposition the protective force. As the test window opens, the protective force will be in its normal operational configuration, with no increased or heightened state of readiness.

7.0

Design Basis Threat and Adversary Team Capabilities

The capabilities attributed to the adversary team for Security Evaluations performance tests will be within the scope of the Design Basis Threat and appropriately approved local threat statements (if any) unless otherwise agreed. Security Evaluations may use all adversary skills, weapons, equipment, and other attributes that can be inferred from the Design Basis Threat.

Security Evaluations will develop and periodically update a list of weapons,

ammunition, explosives, and other equipment that will be considered a part of the adversary team's inventory. The list will be based on a sample of items generally available in the world. It will be supported by applicable data, obtained from authoritative sources, on accuracy, lethality, destructive force, reliability, etc. Security Evaluations will use that data as the basis for weapons/explosives performance during testing. The list will be published separately as Appendix A to this document, and may be classified.

8.0

Participant Selection

Security Evaluations' goals in selecting performance test participants (Players) is to test a group that is representative of the protective force, and to select participants in a manner that is free from bias. In the case of limited scope tests, the preferred method is to select a random sample from the appropriate population. (The appropriate population may be the entire protective force, special response team, alarm station operators, etc., depending on the test.)

For major performance tests, an entire protective force shift, or that portion of a shift working at the targeted facility, may participate. The specific shift(s) tested will depend upon a number of factors, including the date and time of the test and the established shift work schedule. Security Evaluations will remain flexible in working with the inspected facility to schedule participants so as to minimize schedule disruption and overtime costs. However, Security Evaluations stresses several factors:

- **Realism.** The shifts tested should be operating in their normal environment. For example, a shift that only works days Monday through Friday should not be tested in a nighttime scenario; a shift from one facility should not be tested in a scenario at a facility where they don't normally work.
- **Broad coverage.** When tests are being conducted on more than one day, a different shift should be tested each day.
- **Shift and post integrity.** Only personnel assigned to the tested shift should be tested, and all participants should be assigned to their normal posts/patrols/duties, according to a normal schedule for the shift. Personnel from other shifts should not be substituted, and shift personnel should not be assigned non-routine posts in an effort to improve performance by "hiding" personnel perceived to be weaker performers.

9.0

Safety

Participant safety is an important consideration in planning and conducting Security Evaluations performance tests. Security Evaluations includes a Safety Coordinator as part of its test planning team whose responsibility is to work with assigned facility Safety Coordinators to identify and help mitigate risks associated with testing activities.

Realism is also critical to performance testing and must be preserved to the extent possible. The types of activities being tested often themselves involve inherent risks, such as those associated with operating vehicles, running, negotiating barriers, working in an environment posing various radiological and industrial hazards, and using small arms. However, risk should be minimized while achieving the necessary levels of realism. Security Evaluations' goal is to achieve a reasonable balance so that meaningful tests can be safely conducted.

10.0

References

The following Department of Energy documents contain information of specific pertinence to the general subject of performance testing/exercises.

1. DOE Order 470.1, Safeguards and Security Program, 9-28-95
2. DOE Order 470.2, Safeguards and Security Independent Oversight Program, 12-23-98
3. DOE Order 5480.16A, Firearms Safety, 3-4-94
4. DOE Order 5632.7A, Protective Force Program, 4-13-94
5. DOE Guide 5632.7A-1, Guide for Use of Protective Force Engagement Simulation Systems, 4-10-95