UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

July 7, 1980

Regulatory Guide 5.61

REGULATORY GUIDE DISTRIBUTION LIST (DIVISION 5)

SUBJECT: Regulatory Guide 5.61, "Intent and Scope of the Physical Protection Upgrade Rule Requirements for Fixed Sites"

Regulatory Guide 5.61 is being issued as an active guide. The information that provided the basis for the preparation of the guide was distributed for comment as a draft report to all affected licensees and to other interested parties who attended the NRC Upgrade Rule Guide Seminar held on March 27-28, 1979, in Richmond, Virginia. No comments were received as a result of this distribution. The resulting active guide is being issued so that affected licensees may use it for preparation of their physical protection plans in response to the new requirements of 10 CFR Part 73 published in the Federal Register on November 28, 1979 (44 FR 68184). Since a draft guide was not distributed for comment, copies of this active guide are being sent to all addressees on the Division 5 distribution list. Although comments are always encouraged on all regulatory guides, comments on this guide are particularly encouraged at this time since a draft guide for comment was not published.

Robert B. Minogue

Robert B. Minogue, Director
Office of Standards Development

June 1980

U.S. NUCLEAR REGULATORY COMMISSION

REGULATORY GUIDE

OFFICE OF STANDARDS DEVELOPMENT

REGULATORY GUIDE 5.61

INTENT AND SCOPE OF THE PHYSICAL PROTECTION UPGRADE RULE REQUIREMENTS FOR FIXED SITES

A. INTRODUCTION

On November 28, 1979, strengthened physical protection requirements for fuel cycle facilities and transportation involving formula quantities of strategic special nuclear material were published in the *Federal Register* (44 FR 68184). The "Physical Protection Upgrade Rule" is the short title for these requirements. This guide provides information to assist in understanding the physical security requirements for fuel cycle facilities set forth in §§ 73.1, 73.20, 73.45, and 73.46 of the Physical Protection Upgrade Rule. Section B, "Discussion," provides an overview of the major sections of the rule and discusses (1) how the Physical Protection Upgrade Rule is structured, (2) what the purposes of its major provisions are, and (3) what interrelationships exist among the three major portions of the rule that contain requirements for the physical protection of fixed sites. Section C, Regulatory Position, attempts, by means of a question and answer format, to explain, why certain fixed site requirements are included in the rule and to clarify the intent of these requirements.

B. DISCUSSION

This section is intended to give the reader a broad overview of the structure of the Physical Protection Upgrade Rule as it applies to fixed sites and the purpose of its major provisions. A review of the threat statement is included. The Physical Protection Upgrade Rule is structured in three distinct levels; two are essentially performance oriented and the third, a reference physical protection system, is specification oriented.

1. Purpose and Scope: § 73.1 (Threat Statement)

Paragraphs 73.1(a)(1) and (a)(2) describe the types of threats against which the physical protection system must be effective. Distinctions are made between the overall protection level to be provided against radiological sabotage and that required against theft or diversion of SSNM.

For radiological sabotage, two basic adversary types are defined. The first is an external assault by several persons in which the attackers are assumed to be well armed, well trained, and able to obtain inside help. The second postulated adversary is a single insider who may be employed in any position and who may have an NRC or DOE security clearance.

For theft or diversion, the basic external assault threat is similar to that for radiological sabotage, except that the adversaries are assumed to be capable of operating as two or more teams. The internal theft or diversion threat is markedly different from that for radiological sabotage in that it also includes a conspiracy among individuals either with access to and knowledge of facilities and activities or equipped with items that could facilitate theft of material subject to this rule.

2. General Performance Objective and Requirements: Paragraphs 73.20(a) and (b)

The general performance objective and requirements are referenced to the threat statements of § 73.1, wherein appropriate design basis threats for protecting against radiological sabotage and preventing theft of special nuclear material are specified.

Paragraph 73.20(a) is the first of the two performance-oriented levels and sets forth the rule's basic parameters. This paragraph states who is covered by these regulations; i.e., licensees authorized to operate fuel reprocessing plants pursuant to 10 CFR Part 50, licensees who operate facilities that possess or use formula quantities of strategic special nuclear materials, and licensees involved in the transport or delivery of formula quantities of strategic special nuclear material, including import and export. On an interim basis, non-power reactors are not subject to the Physical Protection Upgrade Rule requirements. It further states that those covered by these regulations must establish and maintain or make arrangements for a physical protection system which

will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

Paragraph 73.20(b) describes how licensees covered by these regulations are to provide effective physical protection systems meeting the general performance objective of paragraph (a) of section 73.20. To meet the general performance objective, a licensee must establish and maintain or arrange for a physical protection system. That physical protection system must include the characteristics defined in paragraphs (b)(1) through (b)(3), which require that the physical protection system (1) provide the performance capabilities of section 73.45, (2) be designed with redundancy and diversity, and (3) include a testing and maintenance program as described therein.

3. Performance Capabilities for Fixed Site Physical Protection: § 73.45

Paragraph 73.20(b)(1) provides a direct link between the general performance requirements and the performance capabilities that comprise the second of the performance-oriented levels. This paragraph states that, in order to meet the general performance requirements of paragraph 73.20(a), a licensee must establish and maintain or arrange for a physical protection system that provides the performance capabilities described in § 73.45 for fixed site protection unless otherwise authorized by the Commission. Thus, a physical protection system must be designed to satisfy the performance capabilities in order to meet the objective of providing high assurance of preventing the theft of SSNM and protecting against radiological sabotage by the previously described adversaries.

Because the adversary may consist of insiders operating alone or in combination with persons without authorized access, the adversary is able to initiate his activities inside as well as outside the facility. In order to provide the required level of assurance, the physical protection system must be able to detect, assess, and respond to unauthorized acts initiated at any point outside or inside the facility. The performance capabilities necessary to provide assurance that the act will be prevented may, therefore, be viewed as a series of four protection layers that detect and respond to an unauthorized act initiated at any point.

Starting from the facility perimeter and working inward, the first protection layer consists of the performance capability delineated in paragraph 73.45(f), which is to provide for authorized access and assure detection of and response to unauthorized penetrations of the protected area. This performance capability is the first line of defense against external groups, but does not provide protection against persons or material with authorized access to the facility. The second protection layer is the performance capability delineated in paragraph 73.45(b), which is to prevent unauthorized access of persons and materials into material access areas and vital areas. This performance capability denies unauthorized access to a material access area or a vital area but is still not effective against adversaries with authorized access to a material access area or a vital area. This problem is addressed by the third layer of performance capabilities delineated in paragraph 73.45(c) which requires that the physical protection system permit only authorized activities and conditions within protected areas, material access areas, and vital areas, and paragraph 73.45(d) which requires that the physical protection system permit only authorized placement and movement of strategic special nuclear material within material access areas. These two performance capabilities ensure that, even in cases in which the adversary is authorized access to material access areas or vital areas and is authorized to handle and move SSNM, the physical protection system will be capable of detecting the unauthorized adversary act and initiating an effective response. The fourth protection layer permits the removal of only authorized and confirmed forms and amounts of strategic special nuclear material from material access areas (paragraph 73.45(e)).

The final performance capability [paragraph 73.45(g)] is that the physical protection system must provide a response capability to assure that the five capabilities described in paragraphs (b) through (f) of § 73.45 are achieved. In cases where the adversary initiates action outside the facility or in the facility's protected areas, he will face redundant protection in the several layers of performance capabilities remaining between him and his objective. But, again, the primary purpose for this layering of performance capabilities is to ensure that an unauthorized act by an adversary will be detected as soon as it is initiated, regardless of who the adversary is or where within the facility he is located.

The proper implementation of these performance capabilities will provide the desired high assurance that the physical protection system can prevent the theft of strategic special nuclear material and protect against radiological sabotage by any of the postulated adversaries at any given time.

4. Fixed Site Physical Protection Systems, Subsystems, Components, and Procedures: § 73.46 (Reference System)

Regulatory guidance to assist in ensuring the proper implementation of the performance capabilities identified in § 73.45 in the design of a physical protection system are contained in § 73.46 and constitute the third major level of the Physical Protection Upgrade Rule. Section 73.46 delineates those safeguards measures that usually will be included in a physical protection system that satisfies the performance capability requirements. In order to clarify the relationship between the reference system in § 73.46 and the performance capabilities in § 73.45, Table 1 has been developed. This table is organized by performance capability, with each capability function and subfunction designated in the rule as necessary to achieve that performance capability listed as a separate column heading. Under each heading are listed all the provisions from the reference system (§ 73.46) that fulfill some portion of that function or subfunction. The table shows how the reference system may be used to provide the functions or subfunctions necessary to each

performance capability and thus to achieve each performance capability itself. The table provides several types of information on how safeguards measures can be used to help satisfy a required function or subfunction. In providing this information, various situations must be considered. For fixed sites, the reference system must consider situational and timing differences (for example, working hours versus non-working hours).

The column headed by paragraph 73.45(b)(2)(ii) provides an example. This paragraph deals with entry controls and procedures for the detection of attempts to gain unauthorized access into material access areas and vital areas by deceit. The paragraphs from the reference system that comprise the body of the column contain components and measures for dealing with entry attempts by employees, non-employees requiring frequent access, visitors, individuals with NRC or DOE material access authorizations, vehicles, and materials. There are also safeguards measures listed for key, lock, and combination control and for communications. Thus, the reference system contains different ways of providing these subfunctions of the performance capability under different circumstances. Some of the activities, equipment, and design features needed to provide the functions and subfunctions are not time sensitive (that is, they must be in effect or be operational at all times). Physical barriers, for example, are not the type of safeguards measure that needs to be effective only at certain times.

To provide this same high assurance of protection over time, paragraph 73.20(b) of the general performance requirements, contains two additional requirements, redundancy and diversity and testing and maintenance.

5. Redundancy and Diversity: Paragraph 73.20(b)(2)

Paragraph 73.20(b)(2) requires that the physical protection system be designed with sufficient redundancy and diversity to assure maintenance of the capabilities described in section 73.45. To provide protection against the failure of physical protection system measures that would cause a performance capability not to be satisfied, the system must be designed with redundancy and diversity. That is, redundant and diverse means of providing functions or subfunctions must be included to ensure that no single adversary act or no single safeguards-measure failure will cause the overall system to fail. Redundancy means providing more than one measure (which may be the same measure duplicated) to perform a given function or subfunction. Diversity means providing two or more different kinds of measures that all perform or contribute to the same function or subfunction but that have different operating characteristics (such as sensitivities, failure modes, strengths, and weaknesses).

Table 1 is useful in clarifying the role of redundancy and diversity in the physical protection system. Paragraph 73.46(g)(5) of the reference system implies that redundancy and diversity are not required everywhere, but only in those cases in which the effectiveness of the physical protection system would be compromised by failure or other contingencies. As stated in paragraph 73.20(b), this means that the physical protection system must be designed with sufficient redundancy and diversity to assure maintenance of the capabilities described in § 73.45. In terms of information provided by the table, this means that components providing redundancy and diversity will not be found in every column, but only in those in which the criteria of the reference system makes their inclusion warranted. Thus, in providing the functions and subfunctions of the performance capabilities as shown through the columns on the table, guidance is given showing the usual level for redundancy and diversity needed to satisfy paragraph 73.20(b)(2).

6. Testing and Maintenance: Paragraph 73.20(b)(3)

Paragraph 73.20(b)(3) requires the physical protection system to include a testing and maintenance program to assure control over all activities and devices affecting the effectiveness, reliability, and availability of the physical protection system, including a demonstration that any defects of such activities will be corrected for the total period of time they are required as a part of the physical protection system. This requirement is intended to ensure that all procedures and hardware will remain effective, reliable, and available at all times. This requires programs to promptly detect any defects and to correct them in a timely manner. It also requires a program to provide alternative measures to replace the capabilities lost while the maintenance and repair is being accomplished.

Testing and maintenance that normally will be included in a system providing the capabilities required by paragraph 73.20(b)(3) are described in paragraph 73.46(g) of the reference system. In order to ensure that required performance capability functions or subfunctions are performed, the reference system provides guidance for a testing and maintenance program. The purpose of any testing and maintenance program should be to ensure continued operation of the safeguards measures that are used to provide those functions or subfunctions.

Table 1 delineates reference system maintenance provisions corresponding to the appropriate performance capabilities of § 73.45.

C. REGULATORY POSITION

This section provides the rationale for and clarifies the intent of particular requirements for fixed sites in the Physical Protection Upgrade Rule.

§ 73.1 Purpose and Scope (Threat Statement)

Q: Is there more concern for theft of SNM than for radiological sabotage?

A: The threat statements reflect the position that there is a greater risk to the public from theft of SNM at a fuel cycle facility than from radiological sabotage because of the type and form of SNM actually located at existing fuel cycle facilities. Therefore, it is necessary for licensees' physical protection systems to provide a level of assurance that is consistent with the higher potential damage to the national security and public health and safety.

TABLE 1

RELATIONSHIP BETWEEN THE FIXED SITE PERFORMANCE CAPABILITIES (§ 73.45) AND THE FIXED SITE PHYSICAL PROTECTION REFERENCE MEASURES (§ 73.46)

73.45(b)

(b) Prevent unauthorized access of persons, vehicles, and materials into material access areas and vital areas. To achieve this capability the physical protection system shall:

(1) Detect attempts to gain unauthorized access or introduce unauthorized material across material access or vital area boundaries by stealth or force using the following subsystems and subfunctions:

(i) Barriers to channel persons and material to material access and vital area entry control points and to delay any unauthorized penetration attempts by persons or materials sufficient to assist detection and permit a response that will prevent the penetration; and

73.46(c)(1)
(g)(1)
(g)(2)
(g)(3)
(g)(4)
(g)(5)

(ii) Access detection subsystems and procedures to detect, assess and communicate any unauthorized penetration attempts by persons or materials at the time of the attempt so that a response can prevent the unauthorized access or penetration.

73.46(c)(4) (g)(2)
(d)(9) (g)(3)
(e)(2) (g)(4)
(e)(3) (g)(5)
(e)(4) (g)(6)
(e)(5) (h)(4)(i)
(e)(7) (h)(4)(ii)
(e)(8) (h)(4)(iii)
(f)(1) (h)(5)
(f)(2) (h)(6)
(f)(3) (h)(7)
(g)(1) (h)(8)

(2) Detect attempts to gain unauthorized access or introduce unauthorized materials into material access areas or vital areas by deceit using the following subsystems and subfunctions:

(i) Access authorization controls and procedures to provide current authorization schedules and entry criteria for both persons and materials; and

73.46(d)(2)
(d)(3)
(g)(6)

(ii) Entry controls and procedures to verify the identity of persons and materials and assess such identity against current authorization schedules and entry criteria before permitting entry and to initiate response measures to deny unauthorized entries.

73.46(d)(1)
(d)(2)
(d)(3)
(d)(9)
(d)(14)
(f)(1)
(f)(2)
(f)(3)
(g)(6)

TABLE 1 (CONTINUED)

73.45(c)

(c) Permit only authorized activities and conditions within protected areas, material access areas, and vital areas. To achieve this capability the physical protection system shall:

(1) Detect unauthorized activities or conditions within protected areas, material access areas and vital areas using the following subsystems and subfunctions:

(i) Controls and procedures that establish current schedules of authorized activities and conditions in defined areas;	(ii) Boundaries to define areas within which the authorized activities and conditions are permitted; and	(iii) Detection and surveillance subsystems and procedures to discover and assess unauthorized activities and conditions and communicate them so that response can be such as to stop the activity or correct the conditions before strategic special nuclear material is stolen or radiological sabotage committed.
73.46(d)(1) (d)(2) (d)(8) (g)(6)	73.46(c)(1) (c)(2)	73.46(c)(3) (c)(4) (d)(8) (d)(10) (d)(11) (d)(12) (d)(13) (e)(2) (e)(3) (e)(8) (e)(9) (f)(1) (f)(2) (g)(1) (g)(2) (g)(3) (g)(4) (g)(5) (g)(6) (h)(4)(i) (h)(4)(ii) (h)(4)(iii) (h)(7) (h)(8)

TABLE 1 (CONTINUED)

73.45(d)

(d) Permit only authorized placement and movement of strategic special nuclear material within material access areas. To achieve this capability the physical protection system shall:

(1) Detect unauthorized placement and movement of strategic special nuclear material within the material access area using the following subsystems and subfunctions:

(i) Controls and procedures to delineate authorized placement and control for strategic special nuclear material;	(ii) Controls and procedures to establish current authorized placement and movement of all strategic special nuclear material within material access areas;	(iii) Controls and procedures to maintain knowledge of the identity, quantity, placement, and movement of all strategic special nuclear material within material access areas; and	(iv) Detection and monitoring subsystems and procedures to discover and assess unauthorized placement and movement of strategic special nuclear material and communicate them so that response can be such as to return the strategic special nuclear material to authorized placement or control.
73.46(c)(1) (d)(11) (d)(12) (g)(6)	73.46(c)(5) (c)(6) (g)(6)	73/46(c)(5) (c)(6) (d)(9) (g)(6)	73.46(c)(5) (c)(6) (d)(9) (d)(10) (d)(11) (d)(12) (e)(9) (f)(1) (f)(2) (f)(3) (g)(1) (g)(2) (g)(3) (g)(4) (g)(5) (g)(6) (h)(4)(i) (h)(4)(ii) (h)(4)(iii) (h)(5) (h)(7)

TABLE 1 (CONTINUED)

73.45(e)

(e) Permit removal of only authorized and confirmed forms and amounts of strategic special nuclear material from material access areas. To achieve this capability the physical protection system shall:

(1) Detect attempts at unauthorized removal of strategic special nuclear material from material access areas by stealth or force using the following subsystems and subfunctions:

(i) Barriers to channel persons and materials exiting a material access area to exit control points and to delay any unauthorized strategic special nuclear material removal attempts sufficient to assist detection and assessment and permit a response that will prevent the removal; and

73.46(c)(1)

(ii) Detection subsystems and procedures to detect, assess and communicate any attempts at unauthorized removal of strategic special nuclear material so that response to the attempt can be such as to prevent the removal.

73.46(d)(9), (d)(10), (d)(11), (d)(12), (e)(2), (e)(3), (e)(5), (e)(6), (e)(7), (e)(9), (f)(1), (f)(2), (f)(3), (g)(1), (g)(2), (g)(3), (g)(4), (g)(5), (g)(6), (h)(4)(i), (h)(4)(ii), (h)(4)(iii), (h)(5), (h)(7), (h)(8)

(2) Confirm the identity and quantity of strategic special nuclear material presented for removal from a material access area and detect attempts at unauthorized removal of strategic special nuclear material from material access areas by deceit using the following subsystems and subfunctions:

(i) Authorization controls and procedures to provide current schedules for authorized removal of strategic special nuclear material which specify the authorized properties and quantities of material to be removed, the persons authorized to remove the material, and authorized time schedule;

73.46(g)(6)

(ii) Removal controls and procedures to identify and confirm the properties and quantities of material being removed and verify the identity of the persons making the removal and assess these against the current authorized removal schedule before permitting removal; and

73.46(d)(1), (d)(2), (d)(10), (d)(11), (d)(12), (g)(6)

(iii) Communications subsystems and procedures to provide for notification of an attempted unauthorized or unconfirmed removal so that response can be such as to prevent the removal.

73.46(e)(5), (e)(6), (e)(7), (f)(1), (f)(2), (f)(3), (g)(1), (g)(2), (g)(5), (g)(6), (h)(4)(i), (h)(4)(ii), (h)(4)(iii), (h)(5), (h)(7), (h)(8)

TABLE 1 (CONTINUED)

73.45(f)

(f) Provide for authorized access and assure detection of and response to unauthorized penetrations of the protected area to prevent theft of strategic special nuclear material and to protect against radiological sabotage. To achieve this capability the physical protection system shall:

(1) Detect attempts to gain unauthorized access or introduce unauthorized persons, vehicles, or materials into the protected area by stealth or force using the following subsystems and subfunctions:

(i) Barriers to channel persons, vehicles, and materials to protected area entry control points; and to delay any unauthorized penetration attempts or the introduction of unauthorized vehicles or materials sufficient to assist detection and assessment and permit a response that will prevent the penetration or prevent such penetration from resulting in theft of strategic special nuclear material or radiological sabotage; and

73.46(c)(1)
(c)(2)
(e)(6)
(e)(7)
(h)(1)
(h)(2)
(h)(3)
(h)(6)

(ii) Access detection subsystems and procedures to detect, assess and communicate any unauthorized access or penetrations or such attempts by persons, vehicles, or materials at the time of the act or the attempt so that the response can be such as to prevent the unauthorized access or penetration, or prevent such penetration from resulting in theft of strategic special nuclear material or radiological sabotage.

73.46(b)(1)
(c)(3)
(c)(4)
(d)(4)
(d)(5)
(d)(6)
(d)(7)
(d)(14)
(e)(1)
(e)(8)
(f)(1)
(f)(2)
(f)(3)
(g)(6)
(h)(1)
(h)(2)
(h)(3)
(h)(4)(i)
(h)(4)(ii)
(h)(4)(iii)
(h)(5)
(h)(6)
(h)(7)
(h)(8)

(2) Detect attempts to gain unauthorized access or introduce unauthorized persons, vehicles, and materials into the protected area by deceit using the following subsystems and subfunctions:

(i) Access authorization controls and procedures to provide current authorization schedules and entry criteria for persons, vehicles, and materials; and

73.46(d)(1)
(d)(3)
(g)(6)

(ii) Entry controls and procedures to verify the identity of persons, materials, and vehicles and assess such identity against current authorization schedules before permitting entry and to initiate response measures to deny unauthorized access.

73.46(b)(1)
(d)(1)
(d)(3)
(d)(4)
(d)(6)
(f)(1)
(f)(2)
(f)(3)
(g)(6)

TABLE 1 (CONTINUED)

73.45(g)

(g) Response. Each physical protection program shall provide a response capability to assure that the five capabilities described in paragraphs (b) through (f) of this section are achieved and that adversary forces will be engaged and impeded until offsite assistance forces arrive. To achieve this capability a licensee shall:

(1) Establish a security organization to:

(i) Provide trained and qualified personnel to carry out assigned duties and responsibilities; and

73.46(b)(1)
(b)(4)
(h)(3)
(h)(6)

(ii) Provide for routine security operations and planned and predetermined response to emergencies and safeguards contingencies.

73.46(b)(1)
(b)(2)
(b)(3)
(g)(6)
(h)(3)

(2) Establish a predetermined plan to respond to safeguards contingency events.

73.46(b)(3)
(g)(6)
(h)(1)

(3) Provide equipment for the security organization and facility design features to:

(i) Provide for rapid assessment of safeguards contingencies;

73.46(e)(1)
(e)(2)
(e)(3)
(e)(4)
(e)(5)
(e)(6)
(e)(7)
(e)(8)
(e)(9)
(g)(1)
(g)(2)
(g)(3)
(g)(4)
(g)(5)
(g)(6)
(h)(6)

(ii) Provide for response by assigned security organization personnel which is sufficiently rapid and effective to achieve the predetermined objective of the response; and

73.46(b)(1)
(b)(4)
(g)(1)
(g)(2)
(g)(3)
(g)(4)
(g)(5)
(g)(6)
(h)(3)
(h)(4)(i)
(h)(4)(ii)
(h)(4)(iii)
(h)(5)
(h)(7)
(h)(8)

(iii) Provide protection for the assessment and response personnel so that they can complete their assigned duties.

73.46(b)(1)
(b)(4)
(g)(1)
(g)(2)
(g)(3)
(g)(4)
(g)(5)
(g)(6)
(h)(6)

(4) Provide communications networks to:

(i) Transmit rapid and accurate security information among onsite forces for routine security operation, assessment of a contingency, and response to a contingency; and

73.46(f)(1)
(f)(2)
(f)(3)
(g)(1)
(g)(2)
(g)(3)
(g)(4)
(g)(5)
(h)(6)

(ii) Transmit rapid and accurate detection and assessment information to offsite forces.

73.46(f)(2)
(f)(3)
(g)(1)
(g)(2)
(g)(3)
(g)(4)
(g)(5)
(h)(2)
(h)(6)

(5) Assure that a single adversary action cannot destroy the capability of the security organization to notify offsite response forces of the need for assistance.

73.46(b)(5)
(e)(4)
(e)(5)
(g)(1)
(g)(2)
(g)(3)
(g)(4)
(g)(5)

Q: Is there any reason why the number of adversaries has not been specified?

A: Yes. Threat analysis has shown that basing defense capabilities on a predetermined number of postulated adversaries can be misleading. Given the dynamic nature of the threat and the significance of behavior as well as resource characteristics in determining adversary effectiveness, it was felt that protection against an adversary with a composite of characteristics across a spectrum of threat levels would constitute a more prudent performance objective.

Paragraph 73.1(a)(1)(i)

Q: Is "hand-carried equipment" intended to include toxic gases and antipersonnel ordinance?

A: It is intended that the term "hand-carried" include incapacitating agents (tear gas, mace, tranquilizers, etc.) but not poisonous gases, and that adversaries will have available to them antipersonnel ordinance (hand grenades, claymore mines, etc.). These two adversary attributes indicate that unprepared guards or other response force personnel may be rendered ineffective either prior to engaging the adversary or much more easily during the engagement. The attributes also imply that response force personnel must have special equipment and receive special training to counter these capabilities.

Paragraph 73.1(a)(2)

Q: Is there any special reason why the adversaries have "the ability to operate as two or more teams?"

A: The ability to operate as two or more teams implies that (1) the adversary may be able to split the response force into several groups, thereby reducing the firepower that the response forces can concentrate in any area during an engagement or (2) the adversary may be able to fix the response force in one location by having one team engage the response force while another team maneuvers and completes the theft mission. This adversary attribute has a potential impact on the number of response force personnel that may be required and the response tactics they may employ.

Paragraph 73.1(a)(1) and (a)(2)

Q: Do the knowledgeable individual who renders inside assistance and the conspirators possess the same adversary attributes as the "small group of external attackers"?

A: It is expected that anyone who supports the adversaries' actions will be capable of acquiring the same training as the most sophisticated members of the adversary's group. However, because of the nature of the level of protection required by these regulations it is not expected that the single insider or the conspirators will have available to them all of the weapons, ordinance, or special tools that are considered the attributes of the "small group of external attackers." However, if the insider is a guard or perhaps an armed response individual, he may possess some of the armament referenced in the rule. The prescribed upgrade rule protective measures should limit the quantity and quality of the weapons and ordinance that can be introduced into a facility prior to initiation of the theft or sabotage sequence.

Paragraph 73.1(a)(2)

Q: Is it the intent of the conspiracy threat statement that the physical protection system provide a capability to prevent collusion between more than two insiders?

A: It is the intent of the regulations that those design features of the physical protection system that are affected by the number of insiders in collusion be effective against two colluding individuals. It is expected that some measure of protection will be afforded against larger colluding groups as a result of those features designed to counteract two colluding individuals. Also, the larger the colluding group, the higher the probability it will be detected.

§ 73.20 General Performance Objective and Requirements

Paragraph 73.20(b)(2)

Q: What is the general scope of the "redundancy and diversity" requirement?

A: The physical protection system must be designed with redundant and diverse measures sufficient to ensure that the system will remain capable of providing the necessary level of protection under adverse conditions causing the failure of some elements of the system.

Redundancy means providing several measures (which may be the same measure duplicated) to perform the same function or subfunction in order to prevent failure of the entire system on the failure of a single measure. The performance of any given capability must not be so dependent on any one measure that failure of that measure prevents adequate performance of the capability.

Diversity means providing different kinds or types of measures that contribute to the performance of a given security function or subfunction. By providing various measures that have differing operating characteristics (sensitivities, failure modes, strengths, and weaknesses), the continued performance of a given capability is ensured regardless of the failure of one such characteristic.

An example of pure redundancy is the use of two microwave perimeter intrusion alarm systems installed in parallel and provided with independent annunciators and power supplies. If one of the two microwave perimeter intrusion alarm systems is replaced with a fence-mounted intrusion detection system, both redundancy and diversity have been achieved.

A more abstract example of redundancy and diversity would be the use of a perimeter intrusion alarm system (any technology) with a low-light-level (LLL) closed circuit protected area television surveillance system equipped

with a motion detection capability. For example, a primary perimeter intrusion detection system could be an infrared (IR) system and a redundant secondary capability would be provided by the motion detection feature of the CCTV system. A tertiary intrusion detection capability would be provided by manual observation of the CCTV monitors. A fourth detection capability could be provided by the guard patrols. Diversity of the perimeter detection capability thus is provided by different types of technology used to detect the intrusion. Further diversity is provided by the fact that the LLL CCTV cameras may be designed to work during the failure of the perimeter lighting system.

Paragraph 73.20(b)(2)

Q: In what manner will the redundancy and diversity requirement aid in the protection against the insider or the conspiracy threat?

A: Whether the threat arises from an insider, a conspiracy, or outsiders, redundancy and diversity provides additional elements that must be overcome by the adversary to steal SSNM or commit radiological sabotage. These additional elements improve protection by requiring, for example, the adversary to spend more time in learning system functions and more time in attempting to disarm or compromise a series of systems instead of just one.

Paragraph 73.20(b)(3)

Q: What is the general meaning of the requirement of a "testing and maintenance program to assure control over activities and devices affecting the effectiveness, reliability, and availability of the physical security system" and "a demonstration that any defects of such activities and devices will be promptly detected and corrected"?

A: The physical protection system should include a testing and maintenance program that addresses all elements of the physical protection system and will ensure that all elements remain operating as they are supposed to and that all elements will operate at all times, including under adverse conditions. Testing means procedures to confirm that the individual measures of the safeguards system are performing as designed and intended and are, therefore, providing the appropriate functions and capabilities. Maintenance means not only the repair or replacement of hardware components, but also the review and possible revision of orders establishing procedures that may be necessary to keep physical security systems and subsystems operating effectively.

The testing and maintenance program should be designed to ensure that failures or defects in safeguards measures will be detected promptly and corrected promptly. Both preventive maintenance and repair capabilities are needed. Correction of failures or defects should not be merely temporary fixes but should remedy the fundamental problem and prevent a recurrence of the failure or defect.

Paragraph 73.20(b)(3)

Q: What is the intent of the need "to assure control over all activities and devices affecting the effectiveness, reliability, and availability of the physical protection system"?

A: It is clear that such security devices as alarms and CCTV must be tested and maintained to ensure reliability and availability. However, it is not so obvious, for example, that, if criticality alarms are activated falsely or illicitly, they pose a significant problem to the integrity of the physical security system. This problem exists because these alarms create the impression of an emergency situation that requires emergency evacuations. These evacuations reduce the level of protection for a period of time and provide paths for adversaries to enter or exit the MAA and remove material through an unprotected portal. Therefore, the testing and maintenance program should ensure that such devices are kept in good working order and that illicit activities can not cause the effectiveness of the physical protection system to be impaired.

Examples of activities that might cause criticality alarms to activate erroneously are (1) setting the detection threshold too low and (2) simulating an alarm condition on the signal lines.

Examples of controls over the above activities that might reduce the probability that these erroneous alarms occur are (1) close supervision by knowledgeable security personnel of the calibration process and (2) placing criticality alarms out of reach where possible, enclosing signal lines in conduits, and tamper protecting detection circuitry.

Paragraph 73.20(b)(3)

Q: What are considered defects of activities and devices?

A: Examples of defects in activities that affect the reliability, effectiveness, and availability of the physical protection system are (1) incomplete guard rounds, (2) improper vault opening or closing procedures, (3) escort duties that are not taken seriously, (4) delay in removal of snow from between perimeter infrared intrusion alarm detectors that are in constant alarm, and (5) failure to properly calibrate portal detectors.

Examples of defects in devices that affect the physical protection system are (1) tamper switches that stick in the closed or secure position, (2) alarm components that do not alarm when they lose power, (3) signal lines that have line supervision that is not functioning according to specifications, (4) exterior equipment enclosures that fill with rain and cause equipment failures because they are not properly waterproofed, and (5) unacceptable degradation in detection performance of alarm systems because of other environmental conditions such as high winds.

Paragraph 73.20(b)(3)

Q: What is a "demonstration that any defects . . . will be . . . detected and corrected"?

A: Examples of effective demonstrations would be procedures that (1) cause tamper switches to be physically activated, (2) cause alarm systems to actually operate on emergency power, and (3) measure line supervision tolerances.

Paragraph 73.20(b)(3)

Q: Does the requirement for a testing program imply the need for adversary type testing?

A: Testing does not imply that the licensee should conduct exercises in which individuals assume the roles and characteristics of adversary groups and attempt to commit adversary actions. Drills in which an alarm is sounded (but for which there is no simulated adversary) and the security force's response times and knowledge of contingency plans are demonstrated constitute an appropriate and effective test method. The manner in which the alarm is caused to sound can be used to test its sensitivity, and the location of the alarm selected can be used to test the adequacy of the alarm display and assessment functions.

Paragraph 73.20(c)(2)

Q: What activities constitute "new construction, significant physical modification of existing structures or major equipment modifications," and what kind of evidence that these activities are actually being planned is necessary to permit a delay in implementation to be authorized?

A: The intent of this provision is to permit a delay in implementing those safeguards measures that require lengthy procurement, installation/modification/construction periods, and testing before they can become an integral part of the physical protection system. The licensee should be prepared to show proof, if requested, in the form of signed contracts that clearly indicate the dates of delivery or completion of the subject components or measures, and the name and address of the vendors and contractors. For every measure in which there is an implementation delay, temporary measures that achieve a comparable level of protection will be expected.

§ 73.45 Performance Capabilities for Fixed Site Physical Protection Systems

Q: Is it necessary for some capabilities to be maintained during both normal and emergency conditions? Which ones are they?

A: The following paragraphs contain requirements to maintain the expressed capabilities during both normal and emergency conditions:

73.45(b)(1) and 73.45(b)(2)
73.45(c)(1)
73.45(e)(1) and 73.45(e)(2)
73.45(f)(1) and 73.45(f)(2)

Paragraph 73.45(b)

Q: Why doesn't this capability statement also include a requirement for preventing unauthorized access of persons and materials into the protected area?

A: Because it has been determined that it is not always possible to prevent the unauthorized access of materials or persons into the protected area (PA). Materials can be passed through or thrown over PA barriers, and an external group can penetrate the barriers before the response force has sufficient time to reach the point of penetration. The PA barrier forms only the first of a series of defense-in-depth systems the adversary must compromise in order to effect SSNM theft or sabotage.

Paragraphs 73.45(b)(1) and (b)(2)

Q: Paragraph 73.45(b)(1) is concerned with adversaries who attempt to gain access or introduce material across MAA or VA boundaries using stealthful or forceful tactics. Is it not reasonable to speculate that adversaries might consider the use of stealth or force to introduce unauthorized materials or gain unauthorized access into an MAA or VA through entry control points?

A: The boundaries referred to in the rule include the entry control points for the purposes of stealth or force.

Paragraph 73.45(b)(2)

Q: How do "entry criteria" differ from "authorization controls and procedures" and "authorization schedules"?

A: Detecting attempts to gain unauthorized access into MAAs or VAs by deceit will require the establishment of access authorization controls and procedures to provide current authorization schedules and entry criteria for both persons and materials. Access authorization controls and procedures constitute the administrative process of determining which persons and materials have a legitimate need to enter a given MAA or VA and at what time or under what conditions this need exists. Current authorization schedules will document for entry control personnel which persons and materials are authorized access and the times or conditions for such authorized access. Entry criteria are the aggregate of many pieces of information to be considered or checked in determining whether or not a person or material is authorized entry to that MAA or VA at that time or under those circumstances.

Paragraph 73.45(b)(2)(ii)

Q: What is the intended meaning of the requirement to verify the identity of materials prior to introduction into an MAA?

A: This requirement is intended to ensure that all materials entering an MAA are searched for contraband and that comparisons of shipping documents with package identification and authorization schedules are made. In the case of receipts of SSNM, this requirement does not imply that the packages of SSNM presented for entry into the MAA must be opened and the SSNM scrutinized, weighed, and analyzed at the entry point by security personnel. Authorization to receive this material must be transmitted to entry control security personnel through channels independent of the shipper. SSNM content may be verified by matching information on the shipping documents with that on the containers. Also required would be some form of verification that the package has not been opened or its integrity otherwise compromised. This can be accomplished by the examination of both the container and the tamper-indicating devices affixed to it.

Paragraph 73.45(c)

Q: What is meant by "unauthorized activities and conditions"?

A: The intent of this capability is to ensure that procedures that are consistent with sound security practices are maintained within the MAAs and VAs. The focus is on the security system detecting, primarily through surveillance, activities and conditions that threaten the security posture within the MAA. Unauthorized conditions include such things as vent grills out of place, holes in walls, and vault doors open when not necessary. Unauthorized activities are those that would lead to unauthorized conditions if the activity is not terminated.

Paragraph 73.45(d)

Q: Is it the intent of this paragraph to bring about substantial changes in material control and accounting practices?

A: The intent of this paragraph is primarily to ensure that strategic special nuclear material is located within an MAA and to recognize that certain uses of the material within the MAA may need to be physically separated to make unauthorized removal more difficult. For example, materials directly usable in a clandestine fission explosive should be stored in a vault when not actively undergoing processing, while fuel elements, fuel assemblies, and certain other materials need not be afforded the same degree of protection because of their form. Furthermore, areas such as processing and packaging areas where the material is handled should be controlled separately to provide additional help in preventing unauthorized removal of the material. A physical protection system can accomplish the intent of this paragraph by performing surveillance activities to detect gross occurrences of unauthorized movement and placement of SSNM. This is not intended to be a sophisticated control of small quantities of SSNM that would be a material control and accounting function. Material control and accounting practices can, however, assist in achieving this capability. These practices help to accomplish this by (1) defining authorized placements and movements of SSNM (which should be done in concert with the physical protection system) and (2) providing procedures for informing the physical protection system of current authorizations for placement and movement of materials within the MAA. This includes the receipt of shipments through MAA portals. Licensees should review their fundamental nuclear material control (FNMC) plans and submit appropriate revisions to them to ensure that the above mentioned activities are covered in their plan.

Paragraph 73.45(e)

Q: What is the intended meaning of the term "confirmed forms and amounts"?

A: Confirming the properties and quantities of material presented for removal, that is, establishing that the material presented for removal is in fact what it is purported to be, does not imply that the packages of SSNM presented for removal from the MAA must be opened and the SSNM scrutinized, weighed, and analyzed at the exit point by security personnel. Confirmation does require controls on the packaging, measurement of contents, and sealing of containers prior to removal. Alternative methods of controlling, packaging, measurement, and sealing are discussed in Regulatory Guide 5.57. Controls also should include procedures that permit the exit control security personnel to determine that the package does in fact contain the material listed on the packing document. This may be accomplished by matching the information on the documents accompanying the SSNM with information on other documents prepared by MBA or ICA personnel or other personnel who certified the packaging of the material. These documents are transmitted to the exit control personnel through channels beyond the control of the individuals making the removal. Also required would be some form of verification that the package has not been opened or its integrity otherwise compromised since the MBA or ICA personnel or inspectors certified the contents. This can be accomplished by the use of packaging containers of such design that their structural integrity (or lack thereof) is readily apparent and that are sealed with tamper-indicating seals (see Regulatory Guide 5.10, " Selection and Use of Pressure-Sensitive Seals on Containers for Onsite Storage of Special Nuclear Material," and Regulatory Guide 5.15, "Security Seals for the Protection and Control of Special Nuclear Material"). Checks on seals should include both seal integrity and seal identification.

Paragraph 73.45(e)

Q: Is it the intent of this capability statement that only the modes of stealth and force will be used by adversaries to remove SSNM through the MAA boundary and that only deceit will be used to remove SSNM through the MAA portal?

A: As with other provisions of the rule, the major concern is for stealthful and forceful attempts to penetrate the MAA boundary (barriers) and deceitful attempts to pass through the portal. An adversary using stealth or force to remove material through a portal would probably select an

emergency exit before he would select an exit control point. However, removal by stealth or force through normal entry control points should be considered in the design and operation of the portal. It is also conceivable that an adversary might attempt to pass SSNM around an SSNM detector by using stealth; however, it is expected that the portal design would prohibit this.

Paragraph 73.45(e)

Q: What is the distinction between the activities of "authorization" and "verification"?

A: Authorization determines what is to be permitted and must occur before the act of verification. Verification is the process of determining whether what is happening is or is not authorized.

Paragraph 73.45(e)

Q: Is it the intent of this requirement to make changes in material control and accounting practices?

A: Compliance with this paragraph may require changes in licensee material control and accounting practices and hence their FNMCs. Measurement and packaging of SSNM is ordinarily performed by either operational or material control and accounting personnel. However, controls that ensure that two people have attested to the contents and witnessed the application of the tamper-indicating seal, for example, may need to be instituted in advance to levy an overall internal control system to meet the intent of the regulation. Although Part 70 presently has requirements for tamper-indicating seals, the purpose was to allow the use of a previous measurement for accountability purposes. In this requirement, the intent is to prevent the theft of SSNM both by a single individual and through collusion. Therefore, additional control over the seals and the seal records may be needed. For example, procedures to provide copies of the seal log to exit control individuals might be developed to ensure that two individuals have attested to the contents and witnessed the affixing of the seal and that both of these individuals did not participate in transferring the material to the exit control point.

Paragraph 73.45(e)(2)

Q: Why not confirm the identity and quantity of strategic special nuclear material "authorized" (rather than "presented") for removal from a material access area?

A: The concern is whether material "presented" for removal conforms with the identity and quantity of SSNM "authorized" for removal. "Confirmation" occurs at the time the material crosses the MAA boundary. "Authorization" must occur before the material is moved to the MAA boundary. "Confirmation" should be conducted immediately before departure of the material to preclude tampering.

Paragraph 73.45(f)

Q: Is the intent of this requirement similar to the MAA and VA access controls called for in paragraph 73.45(b)?

A: It is similar, although the emphasis is on detection rather than prevention. This requirement is intended to detect individuals penetrating the PA or introducing unauthorized materials or vehicles through PA portals. Therefore, specific authorization for such access must be presented to the security guards. This capability will ordinarily be accomplished by intrusion sensors, guard patrols, and remote assessment of the PA boundary and through personnel and vehicle searches at the portals.

§ 73.46 Fixed Site Physical Protection Systems, Subsystems, Components, and Procedures (Reference System)

Paragraph 73.46(a)

Q: Why are the systems, subsystems, components, and procedures delineated in § 73.46 included in the Physical Protection Upgrade Rule if there are already general performance and capabilities requirements?

A: The level of detail in paragraphs 73.46(b) through 73.46(h) is included in order to present examples of the types of systems, subsystems, components, and procedures that would normally be included in a physical protection system having the level of performance required of that system in order to be licensed. The required level of performance is specified in §§ 73.20 and 73.45.

Paragraph 73.46(a)

Q: Is there a reference specification provision in § 73.46 for every capability requirement in § 73.45?

A: Table 1 in Section B of this guide demonstrates that there is at least one example provision in § 73.46 for every capability requirement in § 73.45. Usually, there are several provisions in § 73.46 that apply to each requirement in § 73.45. A more detailed discussion of the relationship between these provisions can be found in Section B.4. of this guide.

Paragraph 73.46(b)(2)

Q: What is the meaning of the phrase "members of the security organization with authority to direct the physical protection activities"?

A: The meaning of the phrase is that someone with specifically designated authority and a member of the security organization, e.g., the Director of Security or the security shift supervisor, must be onsite at all times and ready to direct the necessary physical protection activities.

Paragraph 73.46(b)(2)

Q: What is the meaning of the term "physical protection activities"?

A: The term includes the full spectrum of activities from normal guard force duties, through immediate actions required by a security breach, to reaching response forces and obtaining necessary assistance.

Paragraph 73.46(b)(3)(i)

Q: What is the meaning of the term "other individuals responsible for security"?

A: Other individuals are such management personnel as guard supervisors, response personnel who are not members of the guard force, plant security directors, and plant personnel directors.

Paragraph 73.46(b)(3)(ii)

Q: Who is the "individual with overall responsibility for the security functions"?

A: Generally, the individual to whom overall facility security responsibility is delegated is a corporate Vice President, Plant Manager, or the Plant Director for Security.

Paragraph 73.46(b)(4)

Q: Does this provision mean that licensees must submit separate plans to implement the requirements of Appendix B to Part 73?

A: Separate plans will be required to implement the requirements of Appendix B to Part 73, although these should be related to and coordinated with the security plan prepared in accordance with the provisions of the Physical Protection Upgrade Rule.

Paragraph 73.46(c)(2)

Q: Are vehicle barriers required along the PA perimeter?

A: No. It is not the intent of the regulations to require a PA barrier capable of resisting a forceful entry attempt using a vehicle.

Paragraph 73.46(c)(5)

Q: Does "strategic special nuclear material, other than alloys, fuel elements or fuel assemblies" mean all SSNM that is in the form of powder, liquid, or gas?

A: Yes, it includes SSNM in solid, liquid, or gaseous states.

Paragraph 73.46(c)(5)(i)

Q: Must the penetration time of the vault equal local law enforcement response time or response time of the facility response force?

A: The penetration time should either be equal to or greater than the amount of time necessary to deploy a response force capable of containing and preventing removal of SSNM from the facility by the external assault threat (a small group, well trained, well equipped, able to operate as two or more teams, etc.). Depending on site conditions, the response force with this capability could be an appropriate mix of onsite and offsite personnel.

Paragraph 73.46(c)(5)(iii)

Q: Does the term "significant delay to penetrations" mean that this MAA barrier must be more formidable than those surrounding alloys, fuel elements, or assemblies?

A: Yes. The purpose of this provision is to make it difficult for a conspiracy of individuals within the MAA to breach the barrier without being detected and transfer SSNM to the outside.

Under this provision, all openings in the MAA barrier, such as areas under doors, through-fans, ventilation ducts, and pipe passthroughs, that lead to an accessible area outside the MAA should be completely closed off or specially protected. In addition, the barrier should be constructed of a material that resists cutting, drilling, and puncture by small hand tools or tool substitutes. Where possible, all operations at a facility involving SSNM that has not been alloyed or encapsulated should be consolidated in a single location that meets this barrier provision.

Barriers should be inspected at regular intervals to ensure that a breach is not in process.

The secondary intent of this provision is to provide additional protection of unalloyed and unencapsulated SSNM in process against external assault.

Paragraph 73.46(c)(5)(iv)

Q: Does the term "except when personally attended" mean that components and process equipment containing SSNM do not need to be locked as long as someone is in the MAA?

A: No. The only SSNM that does not need to be under lock is that being processed, handled, worked on, or directly observed by personnel.

Paragraph 73.46(d)(1)

Q: What type of escort is required for a non-employee entering an MAA or VA?

A: Non-employees who require occasional access to an MAA or VA should be escorted by either a member of the security organization or a licensee employee who has current authorization to enter that MAA or VA.

Paragraph 73.46(d)(6)

Q: Is use of x-ray for package search required by the rule?

A: No. X-ray is an acceptable method of conducting package searches but is not the only method. Substantial

technical guidance on alternative methods to accomplish package searches are contained elsewhere in the Physical Protection Upgrade Rule Guidance Compendium.

Paragraph 73.46(d)(8)

Q: Must a member of the guard force provide escort to personnel or vehicles that require an escort to enter the PA or may a designating escort be used?

A: A member of the security force should escort vehicles entering the PA. Individual pedestrians may be escorted within the PA by either a member of the security force or a licensee employee who has current authorization to enter the PA.

Paragraph 73.46(d)(9)

Q: To meet the need for dual exit searches from MAAs, may one of the searches be a visual search or must both use electronic detectors, etc.?

A: Visual searches are not considered sufficient to detect small quantities of concealed SSNM. Electronic SNM detectors should be used for both searches.

Paragraph 73.46(d)(9)

Q: What normally would constitute an acceptable random search?

A: A technique that ensures that each individual could be selected for search each and every time the individual leaves the material access area.

Paragraph 73.46(d)(14)

Q: Does the definition of "termination of employment" include employees who have been transferred to another work site?

A: Yes, it is intended that changes to keys, locks, combinations, and other related equipment should be made whenever an employee is transferred to another work site.

Paragraph 73.46(e)(3)

Q: Does the requirement that an individual other than the alarm station operator have knowledge of the opening of unoccupied vaults or process areas indicate that the individual may be notified some time in advance of the opening?

A: No. The individual should witness the opening, either directly or through an assessment mechanism such as CCTV.

Paragraph 73.46(e)(3)

Q: Is one monitor per each remote CCTV camera required in the CAS and SAS?

A: Not in all cases. Guidelines on appropriate CCTV configurations are provided in NUREG/CR-0543, "Central Alarm Station and Secondary Alarm Station Design," and in NUREG-0178, "Basic Considerations for Assembling CCTV," both of which are contained in the Physical Protection Upgrade Rule Guidance Compendium.

Paragraph 73.46(e)(7)

Q: Does the requirement that the status of all alarms and alarm zones be indicated in the alarm station mean that both the central alarm station (CAS) and the secondary alarm station (SAS) have identical annunciation and alarm control (access, secure, test) capabilities?

A: A discussion of which capabilities should be duplicated between CAS and SAS and how and where to accomplish this is discussed in NUREG/CR-0543, "Central Alarm Station and Secondary Alarm Station Design," contained in the Physical Protection Upgrade Rule Guidance Compendium.

Paragraph 73.46(e)(7)

Q: Is the intent of the rule to require a display board in the CAS/SAS indicating the status of *each* alarm with a visual display?

A: The intent is that the status of each alarm can be independently determined in real time at each alarm station, i.e., no "summary alarms."

Paragraph 73.46(g)

Q: What is the meaning of the term "other physical protection related devices"?

A: Examples of devices included in this term are:

- Emergency power sources
- Lighting, normal and emergency
- CCTV surveillance systems
- Weapons and other guard equipment
- Security vehicles
- Electronic access control devices
- Search equipment
- Duress alarms

Paragraph 73.46(g)(5)

Q: Does the provision for "two individuals working as a team who have been trained in the operation and performance of the equipment" mean the electrician and his apprentice or two separate electricians who do not normally work together?

A: The two individuals could be any employees of the licensee or agents or contractors of the licensee who meet all other requirements for access. Both should be trained in the operation and performance of the security equipment involved to the extent that each could detect an unauthorized alteration of the system by the other.

Paragraph 73.46(g)(5)

Q: Do "performance verification tests" differ from "operational tests"?

A: Performance verification tests are an abbreviated form of operational tests. Operational tests are rigorous and systematic tests conducted on every zone of every alarm system at prescribed intervals. Performance verification tests involve testing the performance characteristics of only those functions that were likely to be affected by the maintenance activities in question.

Paragraph 73.46(g)(6)

Q: Does the provision for "individuals independent of both security management and security supervision" mean that someone outside the security program must conduct the review?

A: Yes, the intent is to have a management review by persons other than those responsible for the security programs.

Paragraph 73.46(h)(3)

Q: What is the minimum composition of the response force and other armed personnel that should be available to cope with safeguards contingencies?

A: This provision envisions five armed guards totally committed to the physical security effort being available for response and assessment of safeguards contingencies. The number of "additional" guards or other appropriately trained (in accordance with Appendix B) and armed personnel who must also be available for backup cannot be predetermined on a generic basis. This must be done on a site-by-site basis, giving due consideration to such factors as (1) the size, location, competence, and reliability of the local law enforcement agency; (2) the ease or difficulty with which the site can be approached undetected; (3) the ease with which escape from the site can be made; and (4) the general attitude of the local population toward the site and its management. These are the kinds of considerations that should influence the licensee's determination of the number of available armed personnel as expressed in the physical protection plan.

Paragraph 73.46(h)(3)

Q: May guards and armed response personnel have other duties or must they be dedicated to the response function?

A: Guards and armed response personnel can have other duties as long as such duties do not interfere with their response to a safeguards contingency. Normally, it is expected that the response force would be made up of guards who have routine duties other than response, other members of the licensee's organization who are qualified and trained in accordance with Appendix B, and guards from the licensee's organization who may be located at a facility that is adjacent to the protected area. Guards manning the alarm stations have continuing duties in case of an assault and are not considered to be part of the response force.

Paragraph 73.46(h)(6)

Q: What are some of the measures that can be used to "facilitate the initial response to detection of penetration of the protected area and assessment of the existence of a threat"?

A: To facilitate prompt assessment and initial response to the detection of questionable activity at or in the vicinity of the protected area perimeter, a capability of observing the isolation zones and the physical barrier should be provided. Such means as closed-circuit television (CCTV), hardened observation posts, armored response vehicles, and various combinations of these might be used. The employment of such physical security systems should be governed by the following considerations.

1. CCTV. Coverage should include the entire perimeter, isolation zones, and, to the extent possible, the clear areas between barriers. Cameras on remotely controlled pan and tilt mechanisms may be used for optimum effectiveness. If, however, fixed position cameras are used, the field of view normally would not need to extend beyond the isolation zones. Such limitation should allow concentration within the areas of primary concern. Low-light-level CCTV cameras are most desirable for this purpose owing to their effectiveness during periods of reduced visibility.

2. Hardened Observation Posts. Hardening should be to a level at least equivalent to that of the alarm stations. Such posts should be located so that an unobstructed view of the perimeter and isolation zone that is supposed to be monitored is available. The posts should also have direct communication and alerting capability with the alarm stations, including duress alarms, in order to avoid delay in the transmission of information concerning any threatening event.

3. Armored Response Vehicles. Such vehicles should be armored to a level at least equivalent to that of the alarm stations. They should be capable of reaching a defensive position at any part of the perimeter barrier. Response to such a position must be sufficiently rapid to prevent intruders from reaching and breaching a second barrier without direct visual contact and opportunity for confrontation by the response force. The vehicles should be equipped with duress codes that can be easily activated through the mobile radio.

Assessment is a continuing process of evaluating the security situation and deciding whether or not conditions that dictate the initiation of a response exist. The assessment functions of security personnel and systems such as that described above are important to the achievement of the objectives of a perimeter protection system. Personnel selected for any of the positions that have an assessment role (e.g., observation posts and alarm stations) should be highly competent and dependable. Furthermore, they

should have the unquestionable authority to alert the response force and, in the case of those within the alarm stations, to request assistance from offsite forces.

Paragraph 73.46(h)(7)

Q: Why are security personnel assessing alarms within unoccupied vaults and unoccupied material access areas containing unalloyed or unencapsulated SSNM required to use only remote means to assess these alarms?

A: There are two reasons for this provision. First, to maintain the designed delay time built into vaults, the doors should be kept closed and locked, especially at night and during off shifts. The remote assessment would preclude an adversary from intentionally using a false alarm as a means of getting the vault opened. Second, the use of remote assessment techniques prevents the two responding guards from having access to material access areas and the SSNM. A possible alternative would be to use a team of personnel (more than two) to investigate the source of the alarm.

D. IMPLEMENTATION

This section provides information to applicants and licensees regarding the staff's plans for using this regulatory guide.

Except in those cases in which the applicant proposes an acceptable alternative, after publication of this guide the Commission's staff will use the intents and understandings described herein as one aid for evaluating an applicant's or licensee's capability to conform to the performance-oriented physical protection requirements in the Physical Protection Upgrade Rule.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
U.S. NUCLEAR REGULATORY
COMMISSION