NUREG-0220

INTERIM ACCEPTANCE CRITERIA FOR A PHYSICAL SECURITY PLAN FOR NUCLEAR POWER PLANTS

DRAFT

Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission

NUREG-0220

INTERIM ACCEPTANCE CRITERIA FOR A PHYSICAL SECURITY PLAN FOR NUCLEAR POWER PLANTS

DRAFT

March 1977

Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

TABLE OF CONTENTS

PART I OF THE PHYSICAL SECURITY PLAN ACCEPTANCE CRITERIA

TABLE OF CONTENTS (Continued)

844 192

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

844 194

INTRODUCTION

This document has been prepared for use in conjunction with the "Interim Format and Content for a Physical Security Plan for Nuclear Power Plants", NUREG - 0207, U. S. Nuclear Regulatory Commission, February 1977 (Draft). The presentation of acceptance criteria follows exactly the organization of the "Format and Content" document.

In 10 CFR 73.55 (a) a single criterion for the acceptance of a nuclear reactor physical security system is established. This criterion can be stated succinctly as "high assurance protection against industrial sabotage by a well-armed, team of several outsiders assisted by a single insider or by a single insider acting alone." Satisfaction of this criterion can, of course, be achieved in an infinite variety of ways.

Based upon the requirement for high assurance protection against industrial sabotage and the inherent nature of the nuclear power plant and associated threat, a number of secondary criteria can be derived from the single criterion stated above. These criteria have been derived from the single criterion stated above. These criteria have

been derived to guide the licensee in designing an acceptable physical security system. Additional guidance to the licensee is provided by "Exemplary Design of a Physical Security System for a Nuclear Power Plant" to be published by the USNRC. This exemplary design will be prepared for a generic nuclear power plant using the acceptance criteria stated herein.

The acceptance criteria have been developed in three steps:

1) The general characteristics of nuclear power plants and their physical security systems were established.
2) This description was combined with a general characterization of the threat to produce a set of tactical objectives for the physical security system.
3) The threat was analyzed and the physical security system acceptance criteria appropriate for achieving the tactical objectives for each threat component were obtained.

844 196

PART I OF THE PHYSICAL SECURITY PLAN ACCEPTANCE CRITERIA

CHAPTER 1 - SECURITY ORGANIZATION

1.1 MANAGEMENT ORGANIZATION

Acceptance Criterion 1.1.A

Management of the physical security organization must be independent of the management of the operating organization.

Discussion

This criterion applies to the day-to-day management of physical security and plant operating activities. These activities require coordination which should be provided by establishing independent chains of command reporting to top management of the facility or top corporate management.

Acceptance Criterion 1.1.B

Management of the conduct of physical security audits (See Chapter 14) should be independent of normal physical security management

Discussion

There is a clear conflict of interest when physical security audit procedures are conducted by those whose system is being audited.

1.2 SECURITY ORGANIZATION

844 197

Acceptance Criterion 1.2.A

At least one full time member of the security organization who has the authority to direct the physical security activities of the security organization in meeting the threat shall be onsite at all times. This individual should report directly to the individual

(plant manager, his designated alternate, shift supervisor, etc.) with final responsibility for plant operation on a shift.

Discussion

As will be discussed further in later sections, the nature of the threat is such as to severely limit the amount of outside help that can be provided. Consistent with this philosophy, the criterion calls for the continuous presence of a licensee representative who has the authority to assume overall direction of physical security operations in the event of an incident. This criterion is partially derived from 10 CFR 73.55 (b)(2).

Acceptance Criterion 1.2.B

A clear chain of succession of responsibility must be established for the transfer of authority in the event of disablement of a key member of the physical security organization during an incident.

Discussion

This criterion simply calls for a plan of organization that will permit orderly passage of authority should the individual charged with directing the physical security activities of the security organization be disabled in the course of responding to a security contingency.

1.3 FACILITY PERSONNEL

1.3.1 Personnel Reliability

844 198

Acceptance Criterion 1.3.1.A

The licensee must develop and conduct a screening program for all personnel who are authorized for unescorted access to the protected area. As a minimum, this program should follow the employee screening guidance in American National Standard, ANSI 18.17, "Industrial Security for Nuclear Power Plants". Certification of totally equivalent screening (such as "L" or DOD National Agency Check) by a government program will be acceptable. Personnel routinely on the site should be treated as employees. A contractor screening program is acceptable if it can be proved that the program provides coverage equivalent to or greater than ANSI 18.17.

Discussion

Consistent with federal and state law regarding fair employment practices, a screening program must be developed and administered. This program should exclude from employment those whose background would indicate an inconsistency with the required high level of industrial sabotage protection. As stated in the statement of considerations in 10 CFR 73.55, the Commission is presently considering a screening program.

Acceptance Criterion 1.3.1.B

Assure that the procedures used in potential employee screening are available for USNRC inspection.

Discussion

Records of the procedures of the pre-employment screening program must be maintained in a manner permitting USNRC inspection to assure that the required information is being sought. Private information should be protected consistent with Federal and local "privacy" acts.

1.3.2 Personnel Training in Security Practices

Acceptance Criterion 1.3.2.B

Demonstrate that all authorized individuals (other than physical security force personnel) understand their role in physical security and their responsibility in the event of security contingencies.

Discussion

A training program should be developed to establish and maintain cognizance of physical security procedures by all authorized personnel. A refresher program should be conducted annually. A statement of attendance certified by the instructor shall be considered suitable demonstration.

1.4 PLANT SECURITY PERSONNEL

1.4.1 Qualifications for Employment in Security

Acceptance Criterion 1.4.1.A

All physical security force personnel (guards, watchmen, armed response individuals) must possess physical and mental capabilities consistent with their role in the detection, assessment and neutralization of security contingencies. These qualifications must be checked no less frequently than annually.

Discussion

Refer to "Nuclear Security Personnel Interim Qualification and Training Requirements" for details as to required qualifications and

certifications of compliance. Qualifications are addressed in 10 CFR 73.55 (b)(4).

1.4.2 Screening

No criteria additional to 1.3.1.A and 1.3.1.B.

1.4.3 Training

Acceptance Criterion 1.4.3.A

Provide assurance that all members of the physical security force receive training consistent with their roles.

Discussion

Refer to "Nuclear Security Personnel Interim Qualification and Training Requirements" for details of the required curriculum, qualifications of instructors, and certifications of successful completion. The need for a trained physical security force is established in 10 CFR 73.55 (b)(4).

1.4.4 Retraining

Acceptance Criterion 1.4.4.A

Each guard, watchman, and armed response individual shall be requalified annually. Such requalification shall be documented.

844 201

Discussion

This criterion is established in 10 CFR 73.55 (b)(4). Refer to "Nuclear Security Personnel Interim Qualification and Training Requirements" for details of the required curriculum and certifications of

successful completion.

1.4.5 Security Equipment

Acceptance Criterion 1.4.5.A

All guards must wear distinctive uniforms which clearly distinguish them from nonsecurity and local law enforcement personnel.

Discussion

Uniforms provide identification when responding to security contingencies. It is recommended that uniforms be stored on site to lessen the chance of theft. The requirement for uniforms is established in 10 CFR 73.2.

Acceptance Criterion 1.4.5.B

The guards and armed response individuals must be provided with weapons and equipment consistent with the threat, the requirements of federal and local laws, and the facility's physical security plan.

Discussion

The term weapons as used here includes incapacitating agents, such as Mace. The USNRC recommended weapons and equipment for the guards and armed response individuals are listed in "Nuclear Security Personnel Interim Qualification and Training Requirements". Secure weapons storage should be provided in the protected area. Weapons provided by the licensee or a contractor should not leave the owner-controlled area.

Acceptance Criterion 1.4.5.C

All on-duty physical security force personnel must be capable of continuous communication with the central and secondary alarm stations and will all other members of the security force when within the owner-controlled area.

Discussion

Portable communication equipment should be assigned which minimizes blackout areas. At least two channel transmission and reception will provide an acceptable level of jamming resistance. The communication requirement is derived from 10 CFR 73.55 (f)(1).

1.4.6 Authority of Guards to Use Weapons

There are no specific acceptance criteria.

1.4.7 Security Force Composition

Acceptance Criterion 1.4.7.A

As stated in 10 CFR 73.55 (h)(2) a nominal response force of ten guards and armed response individuals is required. This number must include at least five guards.

Discussion

Any decrease in the number of armed response individuals must be stated here and later justified in Chapter 8.

844 203

1.5 LOCAL AND OTHER LAW ENFORCEMENT AGENCIES

Acceptance Criterion 1.5.A

Demonstrate that a workable response plan has been developed and agreed to in writing by all elements of local and other law enforcement agencies that may be called upon for support.

Discussion

This criterion calls for the establishment of agreements as to how support forces will respond to a call for help and how they will be employed upon arrival.

Acceptance Criterion 1.5.B

Written agreements must be reached with all elements of local law enforcement and other agencies that may be called upon for support in the event of an incident to assure that the direction of physical security operations always rests with a single individual.

Discussion

The instances of authority conflicts in crisis management are numerous. It is desirable, though not necessary, that this authority always rest with a licensee employee. It is necessary that any individual who might assume command be familiar with all aspects of the plant's response plan and the security considerations peculiar to nuclear power plants.

Acceptance Criterion 1.5.C

Demonstrate that key members of appropriate local and other law enforcement agencies have been familiarized with response procedures, plant layout, and the peculiar constraints imposed in the protection of a nuclear reactor.

Discussion

Supporting response personnel must be shown to be familiar with their role in responding to security contingencies.

1.6 ACCESS AUTHORIZATIONS

Acceptance Criterion 1.6.A

Establish definitive, written procedures for granting authorization for protected/vital area unescorted access. These procedures shall satisfy the requirements of ANSI 18.17 and clearly establish the need for access.

Discussion

The number of persons granted unescorted access will clearly affect the possibility of sabotage actions involving authorized individuals. This criterion calls for limiting unescorted access to only those persons requiring access for the safe and efficient operation of the plant. Where feasible, persons requiring access to only a specific vital area should be so authorized. All persons granted unescorted access authorization must have satisfied the requirements of the screening program described in Acceptance Criterion 1.3.1.A.

Acceptance Criterion 1.6.B

Establish definitive, written procedures for granting authorization for protected/vital area escorted access.

Discussion

This criterion calls for the establishment of written procedures to be followed in granting visitors access to protected/vital areas. These procedures should establish that visitors are expected and that they are carrying proper identification.

Acceptance Criterion 1.6.C

All packages and material for delivery into the protected area shall be checked for proper identification and authorization.

Discussion

Procedures must be developed and applied which verify that packages which are mailed or shipped to the plant are expected by the addressee. This criterion is derived from 10 CFR 73.55 (d)(3).

844 206

CHAPTER 2 - FACILITY ENVIRONS

2.1 GENERAL SITE AND AREA LAYOUT

There are no specific acceptance criteria.

2.2 FIXED AND MOBILE SECURITY POSTS IN THE OWNER-CONTROLLED AREA

There are no specific acceptance criteria.

2.3 EARLY WARNING DETECTION SYSTEMS

Acceptance Criterion 2.3.A

If detection systems are used external to the barrier at the protected area perimeter, they must annunciate in both the central and secondary alarm stations. The systems must also be tamper-indicating and self-checking and satisfy any other requirements for intrusion detection systems located at the protected area perimeter.

Discussion

The detection systems considered in this criterion might be used to provide early warning of activities beyond the perimeter of the protected area which might indicate a threat to the protected area. Therefore, fence-monitoring systems or those systems immediately adjacent to the barrier are not to be considered under this criterion. It is required that early warning detection systems satisfy all the requirements established in Chapter 3 for intrusion detection systems located at the protected area perimeter.

CHAPTER 3 - PROTECTED AREA PERIMETERS

3.1 PERIMETER BARRIER AND ISOLATION ZONE

3.1.1 Layout

Acceptance Criterion 3.1.A

Isolation zones maintained in outdoor areas adjacent to the physical barrier at the perimeter of the protected area must extend at least twenty feet on each side of the perimeter and must be free of visual obstructions so as to permit accurate assessment of security contingencies detected at the protected area perimeter.

Discussion

This criterion calls for an isolation zone at the protected area perimeter that permits the assessment system to provide accurate information for all intrusion contingencies.

3.1.2 Physical Barriers

Acceptance Criterion 3.1.2.A

Physical barriers at the protected area perimeter must at the minimum satisfy the requirements of 10 CFR 73.2 (f)(1), (2).

Discussion

The requirement for a barrier at the perimeter of the protected area is established by 10 CFR 73.2 (g).

Acceptance Criterion 3.1.2

Means must be established to prevent unauthorized penetration of the protected area by general and special purpose wheeled vehicles. A system must be established in the isolation zone and within the protected area to derail unauthorized railroad equipment penetrating the protected area.

Discussion

At all points on the protected area perimeter at which successful penetration of the protected area is not prevented by topography or other constraints, a barrier to successful penetration must be established. Successful penetration occurs when the vehicle continues to provide transport after penetration. A tractor-trailer combination should be considered the largest wheeled vehicle seeking to penetrate. Aircraft are excluded.

Acceptance Criterion 3.1.2.C

All security locks should satisfy the criteria stated in 10 CFR 73.2 (m). All security locks, keys, combinations and related equipment must satisfy the requirements of Regulatory Guide 5.12. All security keys should be controlled and kept in a locked cabinet when not in use. Whenever there is evidence that any key, lock, combination or related equipment may have been compromised, it shall be changed. Upon termination of employment of any employee, keys, locks, combinations, and related equipment to which that employee had access shall be changed.

Discussion

The physical security plan must present an effective system for managing all locks, keys, combinations, and other related equipment employed in securing the protected area perimeter. The term "employee" includes both licensee employees and anyone onsite who has had access. This criterion is largely derived from 10 CFR 73.55 (d)(9).

Acceptance Criterion 3.1.2.D

Measures must be taken to fully compensate for any reduction in the effectiveness of a physical barrier

Discussion

Compensatory measures may include steps taken at the protected area perimeter or at other points in the physical security system.

3.1.3 Illumination and Surveillance

Acceptance Criterion 3.1.3.A

Illumination must be maintained at the protected area perimeter including the isolation zone. The minimum level of illumination, as stated in 10 CFR 73.55 (c)(5), is .2 footcandle measured horizontally at ground level.

Discussion

Illumination is sufficient when it permits detection as defined by Acceptance Criteria 3.1.3.B and 3.1.3.C. Loss of illumination is permitted for a maximum of one minute before restoration of illumination.

Initiation of emergency procedures to provide equivalent protection should be started immediately.

Acceptance Criterion 3.1.3.B

High assurance detection of the projection of unauthorized material over the protected area perimeter must be provided.

Discussion

This criterion addresses attempts by the adversary to defeat searches by throwing unauthorized material over the protected area barrier prior to attempted protected area entry through a portal. The presence of unauthorized weapons and explosives within the protected area will provide the adversary an unacceptable tactical advantage.

Acceptance Criterion 3.1.3.C

The capability shall be provided to:

1) Observe unauthorized activities in the isolation zone.
2) Accurately assess intrusion detections made at the protected area perimeter.

Discussion

The first component in this criterion requires that at least one member of the physical security force has the capability of observing unauthorized activities in the isolation zone at all times. This does not require continuous observation. A CCTV system or a manned security post with a field of view in the isolation zone is satisfactory.

The second component requires the ability to clearly view the intrusion zone before the intruder has time to leave the area.

Acceptance Criterion 3.1.3.D

Capability must be provided for transmission of equivalent surveillance data to the central and secondary alarm stations.

Discussion

The requirement for communication of surveillance data obtained by members of the physical security force is satisfied by communications criteria (Acceptance Criteria 3.2.1.7.A and 3.2.2.6.B). Totally equivalent systems for obtaining data from surveillance hardware are not required. What is required is the ability to receive all surveillance data. For example, if there are a number of CCTV cameras at the facility, the central alarm station may have several monitors. At least one monitor is required at the secondary alarm station which has the capability of selecting and displaying the image transmitted by each camera.

3.1.4 Intrusion Detection Hardware

Acceptance Criterion 3.1.4.A

All intrusion detection system hardware must satisfy the criteria of USNRC Regulatory Guide 5.44. The system must provide high assurance detection of all penetrations of the protected area perimeter.

844 212

Discussion

This criterion is based upon the assumption that a high level of detection performance within the protected area (i.e., not near the protected area perimeter) will be inconsistent with efficient operation of the plant. Further, undetected penetration of an armed adversary to a vital area perimeter may provide an unacceptable tactical disadvantage to the physical security system. Consistent with the requirement for proper detection sensitivity stated in Regulatory Guide 5.44, high assurance protection will be provided by the system when it detects an intruder in the secured zone ninety-five out of one-hundred times. The modes of intruder penetration considered should be running, walking, crawling, rolling, and jumping.

Acceptance Criterion 3.1.4.B

All intrusion alarm systems must be provided with emergency electrical power as stated in USNRC Regulatory Guide 5.44.

Discussion

The loss of external power can reasonably be assumed at the start of a violent assault. Alarm systems must be provided by onsite emergency sources with sufficient power to operate.

Acceptance Criterion 3.1.4.C

All intrusion alarm systems must satisfy the criterion for the frequency of false and nuisance alarms stated in Regulatory Guide 5.44. Innocent alarms (defined below) must satisfy the same criterion.

Discussion

False alarms are defined as those alarms which have been generated without any apparent cause. Nuisance alarms are defined as those alarms generated by the alarm system detecting a change in the operating environment. Innocent alarms are caused by animals, authorized personnel, windblown material, etc., entering the security zone.

Acceptance Criterion 3.1.4.D

All intrusion detection systems must be tamper-indicating and self-checking, e.g., an automatic indication is provided when failure of the alarm system or a component occurs, or when the system is on standby power.

Discussion

This criterion is established by 10 CFR 73.55 (e)(2). The requirements for tamper-resistance and self-checking are established by Regulatory Guide 5.44.

Acceptance Criterion 3.1.4.E

All detection system hardware must annunciate at the central and secondary alarm stations. (See also 4.6).

Discussion

This criterion is derived from 10 CFR 73.55 (e)(1).

844 214

Acceptance Criterion 3.1.4.F

In the event of detection hardware outage, compensatory procedures must be developed to assure an equivalent level of protection.

Discussion

Compensatory measures may be taken at any point in the physical security system.

3.1.5 Security Posts (Fixed and Mobile)

Acceptance Criterion 3.1.5.A

If structures considered as defensive positions are established at the protected area perimeter, they must be bullet-resisting. All entrance points to these structures must be locked wher occupied.

Discussion

This criterion refers to structures not at protected area portals. Any structure at the perimeter must be constructed so as to provide the same degree of protection as the remainder of the perimeter barrier. Bullet-resisting is defined in 10 CFR 73.2 (q). The structure must resist an Underwriter's Laboratories Level IV round as defined in UL-752. This is a soft-point round (not armor piercing). Th maximum nuzzle velocity to be considered is 2410 ft/sec.

844 215

Acceptance Criterion 3.1.5.B

The protected area perimeter barrier must be patrolled at the same frequency as the protected area. (See Acceptance Criterion 4.4.B.)

Discussion

The purpose of this patrol is to detect any readily apparent disruptions of barrier integrity and any other unusual occurrences.

3.2 PROTECTED AREA PORTALS

3.2.1 Personnel Access Portals and Posts

3.2.1.1 Layout

Acceptance Criterion 3.2.1.1.A

Access must be through a locked door which is controlled by an individual protected by a structure which is bullet-resistant.

Discussion

This criterion is derived from 10 CFR 73.55 (d)(1). The requirements for bullet resistance are established in Acceptance Criterion 3.1.5.A.

3.2.1.2 Physical Structures

There are no criteria other then those noted in Acceptance Criteria 3.2.1.1.A and 3.1.2.A.

3.2.1.3 Locks, Keys, Combinations and Related Equipment

All locks, keys, combinations and related equipment must comply with Acceptance Criterion 3.1.2.C.

3.2.1.4 Security Posts

844 216

Acceptance Criterion 3.2.1.4.A

Each portal must be manned by at least two members of the physical security force when open for personnel access.

Discussion

All posts will require one person to conduct searches and a second person, in a hardened room (Acceptance Criterion 3.2.1.1.A), to control access. It is desirable, but not necessary, that a guard be within the hardened room.

Acceptance Criterion 3.2.1.4.B

Unauthorized entries must be detected and communicated to the central and secondary alarm stations with a level of assurance consistent with Acceptance Criterion 3.1.4.A.

Discussion

Acceptance Criterion 3.1.4.A established the required level of intrusion detection performance using Regulatory Guide 5.44 as a reference. The same level of intrusion detection must be provided at personnel portals.

Forceful entry at a protected area personnel portal must be detected with high assurance to severely limit the possibility of undetected access to the vital area perimeter. This detection may require the use of duress alarms.

3.2.1.5 Search and Admittance Control Hardware

Acceptance Criterion 3.2.1.5.A

All search and admittance control hardware must annunciate warnings at the portal.

Discussion

All hardware used to detect unauthorized material or personnel seeking unauthorized admittance must annunciate so that members of the security force at the portal are warned. No warning at the central or secondary alarm station is required. Notification of both security force members will reduce the possibility of insider assistance.

Acceptance Criterion 3.2.1.5.B

All packages must be searched prior to protected area entry to detect firearms, explosives and incendiary devices or other items which could be used for industrial sabotage.

Discussion

This search may be conducted using detectors, if these systems can be shown to operate with high assurance. Where high assurance cannot be shown, a physical search must be used including disassembly if necessary. Dogs may be used to search vehicles and packages for explosives if they are trained to Federal Aviation Administration Standards. This criterion is derived from 10 CFR 73.55 (d)(3).

Acceptance Criterion 3.2.1.5.C

A search of all personnel entering protected area must be conducted to detect firearms, explosives, and incendiary devices.

Discussion

All personnel must be searched prior to entry into the protected area. This search may be conducted using detectors, if these systems can be shown to operate with high assurance. Where high assurance cannot be shown, a physical search must be employed. This criterion is derived from 10 CFR 73.55 (d)(1).

844 219

Acceptance Criterion 3.2.1.5.D

Verify the access authorization of personnel entering at protected area portals.

Discussion

In order to assure that unauthorized personnel are not granted protected area access, an effective system for verifying the identity and authorization of each individual must be established at all protected area perimeter personnel portals. This criterion is derived from 10 CFR 73.55 (d)(1).

3.2.1.6 Picture Badge System

Acceptance Criterion 3.2.1.6.A

A numbered picture badge identification system shall be used for all individuals who are authorized access to the protected areas without escort. These badges should show the access authorization level of an individual while in a protected or vital area. An individual not employed by the licensee but who requires frequent and extended access to protected and vital areas may be authorized access to such areas without escort provided that he receives a picture badge upon entrance into the protected area which must be returned upon exit from the protected area and which indicates (i) non-employee no escort required; (ii) areas to which access is authorized and (iii) the period for which access is authorized. Individuals not authorized by the licensee to enter protected areas without escort shall be badged to indicate that

an escort is required and the access authorization level. Badges shall be displayed while inside the protected area perimeter.

Discussion

As a means of personnel control within the protected and vital areas, a system for allowing physical classification of personnel as to their level of access (protected or vital) must be maintained. This permits back-up control of access by all authorized personnel. It is recognized that certain circumstances (e.g., radiation considerations) preclude wearing badges. This criterion is derived from 10 CFR 73.55 (d)(5), (6).

3.2.1.7 Communications

Acceptance Criterion 3.2.1.7.A

Each portal must have the capability of continuous communication with the central and secondary alarm station.

Discussion

This requirement will usually be satisfied by satisfaction of Acceptance Criterion 1.4.5.C which calls for all on-duty physical security force personnel to have continuous communication capability with the primary and secondary alarm stations. It is recommended that wire communications (e.g., telephone, intercom) be provided as a backup.

844 221

3.2.2 Vehicle and Cargo Access Portals and Posts

Acceptance Criterion 3.2.2.A

All vehicles, except under emergency conditions, shall be searched for items which could be used for sabotage purposes prior to entry into the protected area. Vehicle areas to be searched shall include the cab, engine compartment, undercarriage and cargo area.

Discussion

This criterion is derived from 10 CFR 73.55 (d)(4). The requirement for the search of all packages and material transported by vehicles is established by Acceptance Criterion 3.2.1.5.B. All vehicles, whether or not they are licensee-designated, must be searched.

3.2.2.1 Layout

Acceptance Criterion 3.2.2.1.A

Access to the protected area must be controlled by an individual protected by a structure which is bullet-resisting.

Discussion

The level of bullet-resistance required is established in Acceptance Criterion 3.1.5.A.

3.2.2.2 Physical Structures

All structures which are part of the protected area perimeter barrier must satisfy Acceptance Criterion 3.1.2.A.

844 222

3.2.2.3 Locks, Keys, Combinations, and Related Equipment

All locks, etc., must comply with Acceptance Criterion 3.1.2.C.

3.2.2.4 Security Posts

Acceptance Criterion 3.2.2.4.A

All portals must be manned by at least two members of the physical security force when open for vehicle access.

Discussion

All posts will require one person to conduct searches, a second person, in a bullet-resisting room (Acceptance Criterion 3.2.2.1.A), to control access. It is desirable , but not necessary, that a guard be within the hardened room.

Acceptance Criterion 3.2.2.4.B

The number of visitor personnel accompanying a non-licensee-designated vehicle into the protected area should be minimized.

Discussion

The minimum number of personnel required to operate and off-load the vehicle should be permitted protected area access. All those admitted must satisfy the standard criteria established for admittance of visitor (escorted access) personnel.

844 223

3.2.2.5 Vehicle and Cargo Search Hardware

There are no specific acceptance criteria.

3.2.2.6 Commun cations

Acceptance Criterion 3.2.2.6.A

Each portal must have the capability of continuous communication with the central and secondary alarm stations.

Discussion

The discussion of Acceptance Criterion 3.2.1.7.A is applicable and no further discussion is required.

844 224

CHAPTER 4 - PROTECTED AREAS

4.1 LAYOUT

Acceptance Criterion 4.1.A

Exclude storage areas from proximity of vital areas.

Discussion

When material must be transported within the protected area, placing storage areas away from vital area boundaries will reduce the dangers associated with vehicle presence. A further gain will be realized from this procedure through the maintenance of a full field a view of vital area boundaries by elimination of possible obstructions due to the presence of material.

Acceptance Criterion 4.2.B

The physical barrier at the perimeter of the protected area should be separated from any other barrier designated as a physical barrier for a vital area within the protected area.

Discussion

This criterion is contained in 10 CFR 73.55 (c)(2). Sufficient separation (at least 20 feet) must be maintained to prevent bridging from barrier to barrier, thereby avoiding interaction with the perimeter barrier detection systems. Lesser distances will be satisfactory if suitable compensatory measures are provided.

4.2 PHYSICAL STRUCTURES

There are no specific acceptance criteria.

4.3 ILLUMINATION AND SURVEILLANCE

Acceptance Criterion 4.3.A

Illumination must be maintained throughout the protected area including the top and sides of all structures. The minimum level of illumination, as stated in 10 CFR 73.55 (c)(5), is .2 footcandle measured horizontally at ground level.

Discussion

This criterion calls for an extension of the level of illumination required by Acceptance Criterion 3.1.3.A throughout the protected area. Loss of illumination is permitted for a maximum of one minute before restoration of illumination. Initiation of emergency procedures to provide equivalent protection should be started immediately. Illumination measurements for the tops of buildings should be taken there.

Acceptance Criterion 4.3.B

If surveillance hardware systems are provided in the protected area, capability must be provided for transmission of equivalent surveillance data to central and secondary alarm stations.

Discussion

The discussion of Acceptance Criterion 3.1.3.D applies. No additional discussion is required.

4.4 SECURITY POSTS (FIXED AND MOBILE)

Acceptance Criterion 4.4.A

All physical structures in the protected area credited as defensive positions for response forces must provide:

1) Bullet-resistance
2) Full field of view and fire in assigned response area.
3) Audible and visible indication of intrusion alarms in assigned response area.

Discussion

Defensive positions may significantly increase the effectiveness of the response force. It is recommended that these positions be equipped with wire communications to provide a backup to the portable communication system carried by the armed response force.

Acceptance Criterion 4.4.B

All exterior parts of the protected area must be patrolled at random intervals for the purpose of human, on-the-scene visual observation. Each part of the protected area must be observed at least once every two hours. Patrolling personnel must be capable of continuous communication with the central and secondary alarm stations. Procedures must be established for frequent status reporting to the central alarm station.

Discussion

Duress alarms may be used to verify the safety of patrolling personnel. This patrol may be used to satisfy the required observation of vital area boundaries discussed in Acceptance Criterion 5.2.2.A.

4.5 ESCORTS

Acceptance Criterion 4.5.A

Within the protected area the following escort requirements exist:

1) All vehicles not licensee-designated must be escorted by a member of the physical security force (guard, watchman, armed individuals).
2) All visiting personnel must be escorted by an individual who is authorized for nonescorted access to the protected area and designated for escort duty.

Discussion

It is recommended that a guard or armed individual be used to escort vehicles since they might be used to conceal weapons or sabotage material. It is assumed that all weapons and unauthorized material carried by visitors on their persons have been prevented from penetration at the protected area perimeter.

844 228

CHAPTER 5 - VITAL AREA BOUNDARIES

Acceptance Criterion 5.A

Each item on the list of vital equipment shall satisfy the criteria for being designated vital established by 10 CFR 73.2 (i).

Discussion

None required.

Acceptance Criterion 5.B

The licensee shall locate vital equipment only within a vital area which, in turn, shall be located within a protected area such that access to vital equipment requires passage through at least two physical barriers. More than one vital area may be located within a single protected area.

Discussion

This criterion is a restatement of 10 CFR 73.55 (c)(1). It establishes the relationship of vital to protected areas and the minimum essential barrier requirements for vital areas.

Acceptance Criterion 5.C

The licensee shall positively control all points of personnel and vehicle access into the vital areas. Access to vital areas shall be limited to individuals who are authorized access to vital equipment and who require such access to perform their duties. Access to vital areas for the purpose of general familiarization and other non-work-related activities shall not be authorized except for good cause shown to the licensee.

Discussion

This criterion is derived from 10 CFR 73.55 (d)(4). It provides the fundamental guidance for controlling access to vital areas.

There are two elements of positive access control:

1) Assurance of an authorized need for vital area entry
2) Identification that the person actually entering is the individual that has the authorized need for entry.

5.1 LAYOUT

There are no specific acceptance criteria.

5.2 PHYSICAL BARRIERS

5.2.1 Barrier Descriptions

Acceptance Criterion 5.2.1.A

All vital area barriers should be resistant to penetration by explosives and breaching tools. The amount of resistance to penetration must be consistent with the time required for armed force response. The penetration resistance of the barriers must not be diminished by doors, windows, and other openings in the barrier.

Discussion

This criterion applies to all elements, both portal and nonportal, of the vital area barriers located at the vital area boundary.

Acceptance Criterion 5.2.1.B

All emergency exits in vital area barriers should be locked and alarmed.

Discussion

This criterion is derived from 10 CFR 73.55(e)(3). Locks on emergency exits should in no way impede egress from the vital area.

Acceptance Criterion 5.2.1.C

Locks, keys, combinations, and other related equipment should satisfy Acceptance Criterion 3.1.2.C.

Discussion

Locks, keys, combination, and other related equipment used at the vital area boundary should satisfy the criteria for quality and control specified for such equipment used at the protected area perimeter.

5.2.2 Intrusion Detection Hardware

Acceptance Criterion 5.2.2.A

High assurance detection must be provided for all vital area entries. Activ alarm systems must be used to protect portals to unoccupied vital areas. Alarm systems must satisfy the requirements of the "Interim Federal Specification: Alarm Systems, Interior, Security, Components for", W-A-00450-B (GSA-FSS).

Discussion

The physical security system must detect all penetrations of the vital area perimeter whether or not those entries are made at vital area portals. This criterion applies to forceful entries as well

as those that are undertaken by stealth or deceit. This criterion is based upon the conviction that undetected vital area penetration will provide an unacceptable tactical advantage to the adversary. Satisfaction of the criterion may be achieved by inspecting vital area boundary barriers at a frequency consistent with the minimum time or threat penetration using tools authorized for the protected area. This inspection may be conducted by the individual patrolling the exterior locations in the protected area.

Detector and line supervisory units should satisfy specifications included in the Interim Federal Specification W-A-00450-B (GSA-FSS). W-A-00450-B has specifications for three other types of detector units and one type of line supervisory unit which the NRC does not recommend for use by the licensee because of the ease by which they can be bypassed. These are Type II, "Conductive foil," Type VII, "Vibration detector," Type XI, "Pressure mat detector," and the Class AB, "Digital and Tone-Wire Transmitted" line supervisory unit.

The requirement for active alarms is derived from 10 CFR 73.55 (d)(4).

Acceptance Criterion 5.2.2.B

All alarm systems must be provided with standby electrical power.

Discussion

The loss of external power can reasonably be assumed at the start of a violent assault. The transfer of standby power must comply with Interim Federal Specification W-A-00450-B (GSA-FSS).

Acceptance Criterion 5.2.2.C

All intrusion alarm systems must satisfy the criteria for the frequency of false and nuisance alarms stated in Regulatory Guide 5.44 and Interim Federal Specification W-A-00450-B (GSA-FSS).

Discussion

The discussion of Acceptance Criterion 3.1.4.C applies, and no further discussion is required.

Acceptance Criterion 5.2.2.D

All intrusion detection systems must be tamper-indicating and self-checking, e.g., an automatic indication is provided when failure of the alarm system or a component occurs, or when the system is on standby power.

Discussion

This criterion is established by 10 CFR 73.55 (e)(2). The requirements for tamper-indication and self-checking are established by Regulatory Guide 5.44 and W-A-00450-B.

Acceptance Criterion 5.2.2.E

All detection system hardware must annunciate at the central and secondary alarm stations.

Discussion

This criterion is derived from 10 CFR 73.55 (e)(1).

Acceptance Criterion 5.2.2.F

In the event of detection hardware outage compensatory procedures must be developed to assure an equivalent level of protection.

Discussion

Compensatory measures may be taken at any point in the physical security system.

5.3 VITAL AREA PORTALS

5.3.1 Personnel Access Portals and Posts

5.3.1.1 Layout

Acceptance Criterion 5.3.1.1.A

Access to vital areas must be through a locked door. If an individual is controlling access, whether or not he is located at the portal or remote from it, he must be protected by a structure which is continuously locked, is bullet-resistant and permits detection and communication of forceful entry with high assurance.

Discussion

All access to vital areas must be governed by positive access control. There must be high assurance that warnings of attempts to enter vital areas by attacking manned security posts will be communicated to the central and secondary alarm stations. This detection may take the form of duress alarms.

844 234

5.3.1.2 Physical Structures

There are no specific acceptance criteria.

5.3.1.3 Locks, Keys, Combinations and Related Equipment

All locks, keys, combinations and other related equipment must comply with Acceptance Criterion 3.1.2.C.

5.3.1.4 Security Posts

There are no criteria additional to Acceptance Criterion 5.3.1.1.A.

5.3.1.5 Access Control Hardware

Acceptance Criterion 5.3.1.5.A

All access control hardware must annunciate warnings of unauthorized entry attempts at the central and secondary alarm stations.

Discussion

All access control hardware, such as key card systems, must provide redundant warning of unauthorized entry attempts.

5.3.1.6 Coded Badge System

Acceptance Criterion 5.3.1.6.A

Specially coded numbered badges shall be issued indicating vital areas to which access is authorized.

Discussion

This criterion is derived from 10 CFR 73.55 (d)(4). This badge may be the same as the picture badge discussed in Acceptance Criterion 3.2.1.6.A.

844 235

5.3.1.7 Communications

Acceptance Criterion 5.3.1.7.A

Each post at a vital area boundary portal must have continuous communication capability with the central and secondary alarm stations.

Discussion

This requirement will be met by satisfying the requirements of Acceptance Criterion 1.4.5.C.

5.3.2 Vehicle Access Portals and Posts

5.3.2.1 Physical Structures

There are no requirements additional to those of Acceptance Criterion 5.2.1.A.

5.3.2.2 Security Posts

Acceptance Criterion 5.3.2.2.A

A portal must be manned by at least one armed member of the physical security force when open for vehicle access.

Discussion

Because of possible insider complicity, the armed member of the physical security fource escorting the vehicle does not count in the required manning of vehicle portals. The armed escort must remain with the vehicle while in the vital area.

844 236

5.3.2.3 Communications

Acceptance Criterion 5.3.2.3.A

Each fixed security post at a vehicle access portal must be capable of continuous communication with the central and secondary alarm stations.

Discussion

This requirement will be met by satisfying the requirements of Acceptance Criterion 1.4.5.C.

CHAPTER 6 - VITAL AREAS

6.1 CENTRAL ALARM STATION

Acceptance Criterion 6.1.A

The onsite central alarm station shall be considered a vital area.

Discussion

This criterion, taken from 10 CFR 73.55 (e)(1), establishes the central alarm station as a vital area.

6.1.1. Location and Layout

Acceptance Criterion 6.1.1.A

The onsite central alarm station shall be located within a building such that the interior of the central alarm station is not visible from the perimeter of the protected area. This station shall not contain any operational activities that would interfere with the execution of the alarm response function.

Discussion

This criterion, taken from 10 CFR 73.55 (e)(1), establishes the basic location and layout requirements for the central alarm station. The interior must not be visible from the vantage point of an individual standing on the ground (topography should be considered) outside the protected area perimeter.

844 238

6.1.2 Physical Structures

Acceptance Criterion 6.1.2.A

The walls, doors, ceiling, floor, and any windows in the walls and doors of the onsite central alarm station shall be bullet-resisting.

Discussion

The term "bullet-resisting" is to be interpreted as defined in Acceptance Criterion 3.1.5.A. Any hardware associated with doors and windows must also be bullet-resisting.

Acceptance Criterion 6.1.2.B

All portals (windows, doors) which would permit personnel entry (aperture area exceeding 96 sq. in. or one dimension exceeding 6 inches) must be kept locked at all times.

Discussion

Locks, keys, combinations, and other related equipment used must satisfy Acceptance Criterion 3.1.2.C. They should be designed so as to impede only entry to the central alarm station.

6.1.3 Alarm and Surveillance Monitoring Hardware

Acceptance Criterion 6.1.3.A

All alarms should annunciate within one second in a continuously manned central alarm station located within the protected area. Alarm hardware should satisfy the requirements of W-A-00450-B.

Discussion

This criterion is derived from 10 CFR 73.55 (c)(1) and defines the basic function of the central alarm station. Use of the processing capability of a computer to support nonsecurity functions should not interfere with the ability to support security functions.

Acceptance Criterion 6.1.3.B

The annunciation at the onsite central alarm station shall indicate the type of alarm (e.g., intrusion alarm, emergency exit alarm, etc.) and location. The central alarm station operator must not be able to change any alarm point status (SECURE, ACCESS, or INOPERATIVE) or actuate any locking or controlling device at a protected area or vital area portal without first getting an enabling action from the secondary alarm station operator.

Discussion

This criterion is derived from 10 CFR 73.55 (e)(2). The degree of alarm localization must be integrated with the planned capability to assess and respond to the alarm.

Acceptance Criterion 6.1.3.C

The central alarm station must be capable of performing all required operations on emergency power.

844 240

Discussion

The loss of all external power at the start of a violent assault is a reasonable assumption. This criterion calls for full operational capability to exist within the central alarm station from the time primary power is lost with no interruption. This emergency power should be provided from onsite sources.

Acceptance Criterion 6.1.3.D

All annunciator and other alarm or surveillance system hardware, including transmission lines, shall be tamper-indicating and self-checking.

Discussion

The criterion is based on standards established for all detection aids in 10 CFR 73.55 (c)(1). Computerized systems should have measures to protect access to computer programs.

6.1.4 Manning

Acceptance Criterion 6.1.4.A

The central alarm station must be continuously manned by at least one member of the physical security force who is totally dedicated to the duties of security monitoring.

Discussion

The importance of the central alarm station in the physical security system prohibits distractions that will result if other

duties are required. The requirement for manning by a security force member, who is not necessarily armed, is based upon the need for monitoring by an individual who is thoroughly familiar with the operation of the physical security system.

6.1.5 Communications

Acceptance Criterion 6.1.5.A

The central alarm station must provide wire (e.g., telephone) and wireless (e.g., radio, microwave) systems which provide fully independent and redundant communication with local law enforcement and the plant control room (s) (if independent of the central alarm station). Capability must also be provided to remain in continuous contact with members of the physical security force while on patrol.

Discussion

This criterion is derived from 10 CFR 73.55 (f)(1), (2), (3). All intermediaries in a communication link must have standby power available. If a communication link is wireless, the entire link must be wireless.

6.2 SECONDARY ALARM STATION

Acceptance Criterion 6.2.A

All alarms shall annunciate in a continuously manned central alarm station located within the protected area and in at least one

other continuously manned station, not necessarily onsite, such that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm.

Discussion

The above statement, derived from 10 CFR 73.55 (e)(1), establishes the requirement for a secondary alarm station. When located onsite this station is to be protected as a vital area. The station must be manned by a not necessarily armed member of the physical security force. Bullet-resistance is not mandatory.

Acceptance Criterion 6.2.B

The secondary alarm station operator must not be able to change any alarm point station (SECURE, ACCESS, or INOPERATIVE) or actuate any locking or controlling device at a protected area or vital area portal without first getting an enabling action from the central alarm station operator.

Discussion

None required.

Acceptance Criterion 6.2.C

Whether or not the secondary alarm station is located onsite, it must satisfy the following requirements:

1) Contains no operational requirements which would interfere with the execution of the alarm response function.

2) Has each personnel entry portal locked at all times.

3) Has annunciators, and other alarm or surveillance hardware which are all tamper-indicating and self-checking.

4) Is capable of fully independent and redundant communications with local law enforcement and the plant control room (if independent of secondary alarm station) and is capable of continuous communication with the physical security force.

6.3 OTHER VITAL AREAS

Acceptance Criterion 6.3.A (Alternate 1)

All access to the very limited number of vital locations, such as containment, wherein acts conducted entirely within this location could result in industrial sabotage must include at least two personnel authorized for unescorted access to vital areas.

Discussion

A limited number of what might be termed "type 1" vital locations exist in a plant. This vital location is an entire vital area or some section of a vital area which can be reached only by passage through a barrier. Extremely sensitive equipment is located in this location, such that an individual would have the ability to commit industrial sabotage actions using authorized equipment. In these few vital locations of the plant actions must be closely monitored. The nominal method of

monitoring will be the "two-man" rule. In those cases where it can be shown that remote television monitoring coupled with rapid response to unauthorized activities can produce an equivalent level of protection, the "two-man" rule is not required.

Acceptance Criterion 6.3.A (Alternate 2)

Compartments are used to eliminate all possibility of access to vital locations (as defined in Alternate 1).

Discussion

A possible alternative to the use of the "two-man" rule is the elimination of the possibility of a single authorization providing access to a plant location wherein action taken entirely in that location could result in industrial sabotage. This could be accomplished by placing vital equipment in compartments (using, for example, wire mesh cages). Positive access control would be applied to each compartment.

Acceptance Criterion 6.3.B

Develop and document procedures for controlling access while in vital areas to tools and materials which could be used to assist in acts of industrial sabotage.

Discussion

There are a large number of tools and materials used routinely in vital areas which could be used in their normal form or in modified

form to assist in performing acts of industrial sabotage. While recognizing that the total control of all such tools and material is not consistent with the efficient operation of the plant, it is clear that the control of materials such as large machinery and potentially explosive chemicals are mandatory in an effective physical security program.

This criterion requires that each licensee develop a program for controlling potentially destructive material in vital areas. The program will provide material control without significantly degrading efficient plant operation. The program should emphasize good housekeeping procedures and the utilization of limited access storage facilities.

6.3.1 Surveillance Hardware

Acceptance Criterion 6.3.1.A

If used, all surveillance system hardware must be self-checking and tamper-indicating.

Discussion

None required.

Acceptance Criterion 6.3.1.B

If used, surveillance hardware must provide equivalent information to the central and secondary alarm stations.

844 246

Discussion

The discussion of Acceptance Criterion 3.1.3.D is applicable.

6.3.2 Security Posts (Fixed and Mobile)

Acceptance Criterion 6.3.2.A

Consistent with operating constraints, all vital areas should be patrolled by a member of the plant staff such that they are visually inspected at least once each shift.

Discussion

Patrols provide a necessary part of any system of vital area monitoring. This requirement does not apply to areas within containment or other areas where inspection would cause exposure to unacceptable levels of radiation. It also does not apply to areas where inspection would significantly interfere with efficient operation of the plant. It is expected that this criterion can be satisfied by the normal rounds of plant operators. Convenient communication capability to the central and security alarm station (e.g., telephone, intercom) should be provided.

Acceptance Criterion 6.3.2.B

If used, all security posts in the vital area should provide continuous communication capability with the central and secondary alarm stations.

Discussion

This criterion will be met by satisfying Acceptance Criterion 1.4.5.C which requires continuous communication capability to the central and secondary alarm stations for all members of the physical security force.

6.3.3 Escorts

Acceptance Criterion 6.3.3.A

Provide escort for visitor personnel in vital area.

Discussion

All visitor personnel (not authorized for unescorted access) must be escorted by an individual authorized for unescorted access to the protected area and designated for escort duty. The maximum permissible ratio of unauthorized personnel to escort personnel is five to one.

Acceptance Criterion 6.3.3.B

Provide armed escort for vehicles in vital areas.

Discussion

Vehicle access to vital areas is expected to be limited. When access is required, the threat associated with the presence of vehicles should be limited by the continuous presence of armed security force personnel.

844 248

CHAPTER 7 - CENTRAL COMMUNICATIONS SYSTEMS

7.1 TELEPHONE SYSTEM

Acceptance Criterion 7.1.A

Protect with locks and alarms any locations within the plant at which the ability to telephone internally and/or externally could be significantly disrupted.

Discussion

There may be several locations within the plant, such as the main switchboard or communication closets or cabinets, where a saboteur could easily disrupt all or a large portion of the plant's telephone communication capability. These areas should be locked at all times, constructed to prevent personnel entry other than through a door and alarmed when not occupied.

7.2 INTERCOM AND PUBLIC ADDRESS SYSTEM

Acceptance Criterion 7.2.A

Protect with locks and alarms any locations within the plant at which the ability to use the intercom or public address systems could be largely or totally disrupted.

Discussion

This criterion applies only in those cases where intercoms and/or public address systems are used in the plant and taken credit for in the physical security plan for the plant. In those cases where

it does apply, protection similar to that provided for the telephone system (Acceptance Criterion 7.1.A) should be provided.

Acceptance Criterion 7.2.B

All intercom and public address systems should be provided with an onsite source of emergency power.

Discussion

As was the case with the previous criterion, this applies only to those systems which are credited as being part of the physical security system.

7.3 OTHER CENTRAL COMMUNICATION SYSTEMS

The requirements stated in Acceptance Criteria 7.2.A and 7.2.B apply to all other central communication systems which are taken credit for in the physical security plan.

CHAPTER 8 - RESPONSE TO SECURITY CONTINGENCIES

8.1 RESPONSE FORCE AVAILABILITY

Acceptance Criterion 8.1.A

The operational duties of armed response individuals must not interfere with their ability to perform response tasks.

Discussion

The physical security response force may be composed of guards and armed response individuals. Armed response individuals may be assigned operational as well as physical security responsibilities. A clear discussion of all operational duties of armed response individuals and the location of these duties is required. These operational duties must be correlated with all physical security duties and the freedom of all armed response individuals to immediately perform all physical security duties at all times must be demonstrated.

8.2 ASSIGNMENT OF RESPONSIBILITIES

Acceptance Criterion 8.3.A

Demonstrate that security procedures exist which will be used in responding to each of the contingencies stated in Section 8.2 of the Interim Format and Content Document and in the discussion below. The discussion of the procedures must explain when and how the security organization will take action to execute these procedures in response to the following contingencies:

1) Guard Strike or Other Unavailability of the Security Force

2) Disruptions of Internal Order

- Fires or Explosions
- Site Evacuation
- Personnel Disturbance

3) Stated or Perceived Threats to Sabotage

4) Civil Disturbance

5) Suspected or Confirmed Intrusions or Sabotage Attempts

- Alarmed Annunciations
- Discovery of Breached Barriers

6) Discovery of Unidentified Persons in Protected or Vital Areas

7) Discovery of Suspected Sabotage or Sabotage Devices

8) Multiple Loss of Onsite and Offsite Communications

Discussion

The criterion is largely derived from 10 CFR 73.55 (h)(2). It calls for the development of a plan which will effect efficiently the decisions and actions. The discussion must contain:

1) a predetermined set of decisions and actions to satisfy the stated objective.

2) an identification of the data, criteria, procedures, and mechanisms necessary to accomplish the following:

(i) determine whether or not a threat exists

(ii) assess the extent of a threat, if any

844 252

(iii) inform local law enforcement agencies and request assistance if necessary

(iv) interpose members of the armed response force between vital areas and any adversary attempting entry for purposes of industrial sabotage, and

(v) prevent or delay an act of industrial sabotage by applying a sufficient degree of force to counter that degree of force directed at them, including the use of deadly force when there is a reasonable belief that it is necessary in self-defense or in the defense of others.

3) A specification of the individual, group, or organizational entity responsible for each decision and action.

This discussion is not intended to include any actions under any Emergency Plans (Appendix E of 10 CFR 50) that deal with the hazards to public health and safety that are the consequences of the release of radioactive material, even though these releases might result from acts of sabotage.

The Nuclear Regulatory Commission is considering amendments to regulations governing nuclear reactors which would call for the development of a formal contingency plan. The work done in responding to this criterion will be largely applicable to satisfying the need for a formal contingency plan.

844 253

CHAPTER 9 - SPECIAL SECURITY MEASURES DURING REFUELING/MAJOR MAINTENENACE OPERATIONS

Acceptance Criterion 9.A

There will be no increase in the likelihood of successful industrial sabotage during refueling operations.

Discussion

Refueling and the maintenance and repair operations that normally accompany the refueling process may substantially increase the vulnerability of plants to sabotage.

The licensee must demonstrate that he has developed procedures to maintain high assurance protection against industrial sabotage during refueling operations. Such procedures might include the following steps:

1) Keeping to a minimum the number of personnel permitted within containment and the spent fuel pool building, if outside of containment.
2) Employing a system of work authorizations which permit only authorized work to be performed.
3) Using the system of work authorizations to assist in minimizing the number of "visitor" personnel allowed in vital areas at any one time by permitting convenient task sequencing.

All positive access control and escort procedures must be maintained in all vital areas during refueling operations.

Acceptance Criterion 9.B

Implement procedures for inspecting all vital areas and equipment which may have been visited subsequent to the completion of refueling/major maintenance operations.

Discussion

The large number of personnel present and the large number of tasks being performed make difficult monitoring of all activities. In order to compensate for this problem, careful inspection and testing of all vital areas and equipment is required prior to return to normal procedures. Inspection is only required in those cases where access has been granted to the vital area during the refueling/major maintenance operations.

CHAPTER 10 - SPECIAL SECURITY MEASURES DURING CONSTRUCTION OPERATIONS

Acceptance Criterion 10.A

The level of physical protection afforded a plant site must not be diminished by construction operations at any adjacent site.

Discussion

The presence of heavy equipment, tools, and possibly large numbers of personnel some of whom may be routinely performing tasks in the isolation zone creates an increased threat of industrial sabotage. Procedures for the application of hardware and personnel to provide a level of protection equivalent to that which would exist if construction were not present must be provided.

CHAPTER 11 - OVERALL PHYSICAL SECURITY PROGRAM PERFORMANCE

Acceptance Criterion 11.A

Demonstrate that the physical security system satisfies the general performance requirement, that is, it provides high assurance protection against industrial sabotage.

Discussion

In addition to demonstrating compliance with the detailed requirements of paragraphs (b) through (h) of the rule; it is necessary to show that the integrated physical protection system in conjunction with the security organization will provide protection with high assurance against industrial sabotage. The general performance requirement stated in paragraph (a) of the rule has been provided as an aid in assessing the level of protection considered to be adequate and prudent at this time. The integrated physical protection systems and the security organization must be designed, however, to deal effectively and discriminately with an entire range of possible security contingencies. These could range from the normal situation of no attempt to intrude, to the unknowing and accidental intrusion of a child or adult, to several activists moderately prepared and motivated to intrude in order to vandalize or disrupt operation, to the threat level of §73.55 (a)(1).

844 257

This criterion requires the demonstration that the previously described physical security elements, when integrated to constitute a system, provide high assurance protection against all threat scenarios. While it is not necessary to use the approach described in the following paragraphs in demonstrating high assurance protection, it is strongly recommended since it is conceptually straightforward and will simplify the process of assuring compliance with 10 CFR 73.55.

The approach is based upon the supposition that there are four discrete opportunities to initially detect the threat: (1) beyond or at the protected area perimeter, (2) within the protected area, (3) at a vital area boundary and (4) within a vital area. Given this initial detection there is some likelihood that the threat will be subsequently neutralized. The state of the art in quantifying the performance of detection hardware and procedures has advanced to the point that it is possible in most cases to assign a reasonably precise quantitative value to an associated probability of successful detection. Therefore, the licensee is required to assign such a value and justify the choice. However, rigorous determination of the overall likelihood that the threat will be neutralized, given initial detection, is complex in that it is a function of the adversary tactics, e.g., targets, paths through the facility, etc., the delay afforded by plant barriers, the time of response by the security force and the

engagement between the adversary force and the security force. Some of the variables may be quantified, e.g., delay times afforded by specific barriers and time of response. Others, e.g., probability of armed response force success in an engagement with an adversary involving the use of weapons, cannot be quantified with satisfactory precision using state-of-the-art computational techniques.

Therefore, in general, it must be demonstrated that given initial detection, the onsite response force must be able to intercept and engage an adversary force in less time than is available for the adversary force to successfully penetrate any single or multiple vital area barriers such that disablement of equipment within those areas would lead to a significant release of radioactivity. This demonstration must consider minimum distances (in time) which the adversary must travel, times of delay in penetrating barriers, and times of response by security force personnel. Delay and response time determinations begin with detection of the attempted intrusion. These calculations would include, for example, the determination of

1) Barrier penetrations times
2) Time for the intruder to traverse the shortest available path from the perimeter barrier to the vital area barrier.
3) Times for receiving alarm.
4) Time for threat assessment and response force initiation.
5) Time for the security force response to the intrusion.

In evaluating overall "success" it may be assumed that the ability to engage the adversary force with a superior number of guards and armed response individuals will provide the requisite high assurance of success against the postulated threat. It has been assumed that the original response force will be rapidly reinforced. This assumption should be verified by the licensee's physical security plan.

A simple approach for this demonstration when dealing with the external threat is recommended by the NRC. First high assurance detection (≥.95, see Acceptance Criterion 3.1.4.A) at the protected area perimeter must be shown. Neutralization of the threat is then accomplished if there is successful armed security force response where the criterion for "success" is as established in the previous paragraph. The contributions due to detections at points other than the perimeter can then be ignored.

This is clearly a conservative approach. Credit will be given for the presence of other defenses such as additional barriers within vital area, presence of armed response individuals in vital areas, and the physical separation of vital components.

High assurance protection against the internal threat can be demonstrated by affirming compliance with the Acceptance Criteria which control insider access to protected and vital areas and activities in vital areas.

Acceptance Criterion 11.B

All credit taken for adversary delay (including penetration prevention), intrusion detection system performance, surveillance system performance, search and admittance control hardware performance, and access control hardware performance must be justified. Justification must also be provided for credit taken for the detection performance of humans or animals and the response time performance of the armed response force and supporting law enforcement.

Discussion

The physical security plan must justify by stating references used or tests performed in determining the level of system effectiveness. This justification should consider in detail all environmental effects (weather, atmospheric transmission, electrical transmission, etc.). Where the intrusion detection system consists of more than one subsystem, the method used in computing the overall level of effectiveness must be explained.

PART II OF THE PHYSICAL SECURITY PLAN ACCEPTANCE CRITERIA

CHAPTER 12 - TESTS, INSPECTIONS AND MAINTENANCE

12.1 PHYSICAL BARRIERS AND ACCESS POINTS

Acceptance Criterion 12.1.A

All physical barriers must be maintained in operable condition.

Discussion

This criterion is derived from 10 CFR 73.55 (g)(1). The term "access points" refers to all apertures in physical barriers that normally serve as personnel and vehicle portals and the means (e.g., locks, gates) that are used to control access at these points. Required is a list of each type of barrier and the inspections that are used to assure integrity. Also required is a list of access control mechanisms, the tests that are used to assure credited performance, the frequency of test conduct, and the condition (s) that would indicate each item out of service. It is recommended that each system be inspected no less than once every seven days.

12.2 ALARMS AND ANNUNCIATORS

Acceptance Criterion 12.2.A

Each intrusion alarm shall be tested for performance at the beginning and end of any period that it is used for security. If the period of continuous use is longer than seven days, the intrusion alarm shall be tested at least once every seven days.

844 262

Discussion

This criterion is quoted directly from 10 CFR 73.55 (g)(2). The term "alarm" is defined to include all sensors, transmission lines, and annunciators that comprise the alarm system. Required is a list of each type of alarm system, the functional test that is used to assure credited performance, test frequency, and the conditions that would indicate each item out of service. Also required for each type of alarm system is the calibration test frequency and a commitment to adjust the test frequency in accordance with the demonstrated equipment performance.

12.3 SPECIAL PURPOSE DETECTORS

Acceptance Criterion 12.3.A

All special purpose detectors used as security related devices or equipment shall be maintained in operable condition.

Discussion

This criterion is derived from 10 CFR 73.55 (g)(1). Included in the category special purpose detectors are all systems used to detect the presence of unauthorized material. Required is a list of each type of special purpose detector, the procedures employed for calibration and control, the test (s) used to assure credited performance, the frequency of test conduct, and the conditions that would indicate each item out of service. Also required for each type of

844 263

special purpose detector is the calibration test frequency and a commitment to adjust the test frequency in accordance with demonstrated equipment performance. We intend to study and evaluate weapon detector inspection and test procedures similar to those used by the Federal Aviation Administration. We are also studying procedures for explosives or incendiary detectors.

12.4 COMMUNICATIONS EQUIPMENT

Acceptance Criterion 12.4.1

Communications equipment required for communications onsite shall be tested for performance not less frequently than once at the beginning of each security personnel work shift. Communications equipment required for communications offsite shall be tested for performance not less than once each day.

Discussion

This criterion is quoted directly from 10 CFR 73.55 (g)(3). It requires that all security-related portable and permanent onsite communication systems, whether or not they are intended for routine or emergency use, must be tested roughly every eight hours. Likewise, all security-related offsite communications equipment must be tested daily. The test program described must include a list of all communication systems tested, the test that is used to assure credited performance, the frequency of test conduct, and the condition (s) that would indicate each item out of service.

12.5 SECURITY PERSONNEL EQUIPMENT

Acceptance Criterion 12.5.A

All security personnel equipment shall be maintained in operational condition.

Discussion

This criterion is derived from 10 CFR 73.55 (g)(1). Included as security personnel equipment are weapons, protective clothing, vehicles and all other items that may be used by guards, armed response personnel, and watchmen which does not involve communications. Initial tests should be performed on all items to assure that they are functionally satisfactory. Recurrert tests are required to be performed only on weapons. Weapons should be inspected daily and tested consistent with the time of requalification of guards and armed response personnel. In no case should the period between testing be more than twelve months. All other equipment should be inspected at least every twelve months. The test and inspection program described should include conditions that would indicate a weapon or other piece of equipment unsatisfactory.

844 265

CHAPTER 13 - SECURITY RECORDS

Acceptance Criterion 13.A

All security records should be retained for a period of at least one year with the following exceptions:

1) Initial qualification tests shall be maintained for the life of the equipment.
2) Maintenance records shall be maintained for a period of five years.
3) Security training records shall be maintained for the period of employment of the individual.
4) Records of access to locks, keys, combinations and other related equipment shall be maintained for period of employment of the individual.

Discussion

A minimum of one year is required for NRC inspection purposes. The first exception is required by the need for the information for continued reference for inspection purposes. The second exception permits review of the performance history of security related equipment. Training records are required to assure compliance with Acceptance Criteria 1.4.3.A and 1.4.4.A. Records of access are required to permit compliance with 3.1.2.C.

13.1 SECURITY TOURS, INSPECTIONS, AND TESTS

Acceptance Criterion 13.1.A

Establish and maintain a system for documenting all routine security tours and inspections, and all tests, inspections performed on physical barriers, intrusion alarms, communications equipment and other security related equipment.

Discussion

This criterion is derived from 10 CFR 73.70 (e). Records should provide a description of the purpose of each tour, test, or inspection and the result. Codes may be used. The physical security plan should briefly describe the data to be recorded, the position (s) of the individual (s) responsible for maintaining the log, and the mechanism to be used in assuring that all data is transmitted and recorded.

13.2 MAINTENANCE

Acceptance Criterion 13.2.A

Establish and maintain a system for documenting all maintenance actions performed on physical barriers, intrusion alarms, communication equipment and other security related equipment.

Discussion

This criterion is derived from 10 CFR 73.70 (e). State differences, if any, in the maintenance recordkeeping program from that described in satisfying Acceptance Criterion 13.1.A.

13.3 ALARM ANNUNCIATIONS

Acceptance Criterion 13.3.A

Establish and maintain a system for recording each alarm, false alarm, alarm check, and tamper indication that identifies the type of alarm, location, alarm circuit, date, and time.

Discussion

This criterion is derived from 10 CFR 73.70 (f). The physical security plan should briefly describe the data to be recorded, the position (s) of the individual (s) responsible for maintaining the log, and the mechanism to be used in assuring that all data is transmitted and recorded.

13.4 SECURITY RESPONSE

Acceptance Criterion 13.4.A

Establish and maintain a system that records details of the response by facility guards, watchmen, and if applicable, armed response individuals to each alarm, intrusion or other security incident.

Discussion

This criterion is derived from 10 CFR 73.70 (f). State differences, if any, in this recordkeeping program from that described in satisfying Acceptance Criterion 13.3.A.

13.5 AUTHORIZED INDIVIDUALS

Acceptance Criterion 13.5.A

Establish and maintain a record of all persons who have been authorized access to protected areas.

Discussion

This criterion is derived from 10 CFR 73.70 (a). The name, address, badge number, inception and expiration date of the authorization, areas to which authorized access is granted and the name of the approval authority should be recorded. The physical security plan should indicate the position (s) of the individual (s) responsible for maintaining these records.

13.6 ACCESS TO VITAL AREAS

Acceptance Criterion 13.6.A

Establish and maintain a record of all persons authorized access to vital equipment and the vital areas to which access is authorized.

Discussion

This criterion is derived from 10 CFR 73.70 (b). State differences, if any, in the recordkeeping program from that described in satisfying Acceptance Criterion 13.5.A.

Acceptance Criterion 13.7.A

Establish and maintain a log indicating name, badge number, time of entry, reason for entry and time of exit of all individuals granted access to a vital area.

Discussion

This criterion is derived from 10 CFR 73.70 (d). The recording of entries and exits of vital areas and reasons for entry is necessary to achieve positive access control. The physical security plan should indicate the position (s) of the individual (s) responsible for maintaining these records.

13.7 NONEMPLOYEE ACCESS

Acceptance Criterion 13.7.A

Establish and maintain a register of visitors, vendors, and other individuals not employed by the licensee who are granted access to the protected area. Each such individual shall be required to register his name, date, time, purpose of visit and employment affiliation, citizenship, and name of individual to be visited.

Discussion

This criterion is derived from 10 CFR 73.70 (c), 73.50 (c)(5), and 73.55 (d)(6). Pursuant to 73.50 (c)(5) an individual provided a picture badge because of frequent and extended protected or vital

area access need not be escorted. The position (s) of the individual (s) responsible for maintaining the register should be included in the physical security plan.

CHAPTER 14 - SECURITY AUDITS

14.1 PROGRAM AUDITS

Acceptance Criterion 14.1.A

Establish and maintain a program for periodically providing management review of the physical security program. This program should include an onsite audit and should focus on agreement between the physical security effectiveness being achieved by personnel, hardware, and procedures and the level established by the approved physical security plan.

Discussion

This review should be conducted by management personnel who are not ordinarily responsible for participation in or direct management of the physical security program. The onsite audit may be conducted by appropriate quality assurance personnel or consultants. Required is an identification of the position (s) of review personnel and an affirmation that written audit reports will be prepared. This affirmation might take the form of an audit report outline which identifies the procedures used to audit the system. The audit should take place no less frequently than annually. This physical security plan should identify the annual publication date of this review plan.