NUREG-0908

Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plans

U.S. Nuclear Regulatory Commission

Office of Nuclear Material Safety and Safeguards

NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 1717 H Street, N.W.
   Washington, DC 20555
2. The NRC/GPO Sales Program, U.S. Nuclear Regulatory Commission,
   Washington, DC 20555
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the NRC/GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free upon written request to the Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

GPO Printed copy price: $4.75

NUREG-0908

Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plans

Manuscript Completed: May 1982
Date Published: August 1982

Division of Safeguards
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

ABSTRACT

This guidance document contains acceptance criteria to be used in the NRC license review process. It contains specific criteria for use in evaluating the acceptability of nuclear power reactor security programs as detailed in security plans.

CONTENTS

CONTENTS (Continued)

1 INTRODUCTION

Each licensee authorized to operate a nuclear power reactor must submit for NRC approval security plans documenting how he will comply with the specific requirements of 10 CFR 73.55. NUREG 0908 has been developed to assist the NRC security plan review process of new or revised plans and licensee development of new or revised plans by outlining specific criteria for the elements of plans. The security plan format used by this document is not required for new plan submittals, but, in the opinion of the NRC, it is an acceptable format. This document is intended to ensure consistency and completeness of plan review. Its use is not intended to replace the judgment of an experienced license reviewer.

Although efforts have been made to ensure completeness of this guidance, certain site-specific situations may occur that are not treated by the document. These cases should be handled on an individual basis by the license reviewer.

Use of This Document

Specific physical security plan criteria are presented in "bullet" format in the order outlined by the Contents. Criteria with a regulatory base (i.e., specifically required by regulations), are so indicated by regulatory references in the left hand margins. Bullets for this category of criteria begin with the phrase: "The security plan shall...." Other bullets that are not explicitly referred to in NRC regulations are referenced as guidelines, NUREG, and/or regulatory guide. They present acceptable ways of achieving the overall performance requirements of §73.55(a). Alternative ways of achieving performance objectives may be acceptable. Bullets for this category of criteria begin with the phrase: "An acceptable security plan/ program/etc. would typically...."

This document also contains criteria for several proposed rulemaking actions. These criteria are indicated by asterisking the proposed regulatory reference in the left hand margins. The licensee is not required to comply with these regulations prior to their effective dates; it is incumbent upon the licensee and license reviewer to maintain an up-to-date awareness of the status of new rule-making actions. Guidelines and NRC guidance documents on these proposed rules will be made available to licensees and reviewers upon finalization. In the interim, present regulations apply.

2 PERFORMANCE OBJECTIVES

§73.55(a)

- The security plan shall confirm that a security organization is established and maintained that 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.

3 SECURITY ORGANIZATION

3.1 Establishment of Security Organization

§73.55(b)(1) · The security plan shall describe the security organization including guards, established to protect the facility against radiological sabotage.

guideline · An acceptable security plan would typically indicate that the security organization does not have any other responsibilities that would conflict with the responsibility to protect against radiological sabotage. Fire brigade duty may be considered as conflicting.

§73.55(b)(3)(i) · The security plan shall describe, by position title, the person responsible for day-to-day administration of the security organization.

guideline · An acceptable security program would typically include watchmen and armed response individuals. It should affirm the existence of such positions and identify their purpose and role in the protection of the facility.

§73.55(b)(1) · If a contract guard force is used, the security plan shall describe a written agreement with the contractor which addresses, as a minimum, the following issues:

(i) the licensee is responsible to the Commission for maintaining safeguards in accordance with Commission regulations and the licensee's security plan.

(ii) the NRC may inspect, copy, and take away copies of all reports and documents required to be kept by Commission regulations, orders, or applicable license conditions whether such reports and documents are kept by the licensee or contractor,

(iii) the licensee affirms to demonstrate the ability of physical security personnel to perform their assigned duties and responsibilities, including a demonstration of the ability of the contractor's physical security personnel to perform their assigned duties and responsibilities in carrying out the provisions of the security plan and regulations, and

(iv) the contractor will not assign any personnel to the site who have not first been made aware of these responsibilities.

3.2 Security Organization Management

§73.55(b)(3) · The security plan shall describe a management system whose purpose is to provide for the development, revision, implementation, and enforcement of security procedures.

guideline · An acceptable security plan would typically indicate the chain of command for security (both site and corporate), and site operations by title.

guideline · An acceptable security plan would typically indicate the point(s) of onsite interface between security and operations by position.

guideline · An acceptable security plan would typically indicate the position onsite with the ultimate security responsibility at all times.

guideline · An acceptable security plan would typically indicate the delegation of authority for security, starting with the position holding the ultimate security responsibility down to the shift-to-shift supervision.

guideline · An acceptable security plan would typically indicate the corporate office to which the onsite security organization can appeal operations/security conflicts.

§73.55(b)(2) · The security plan shall indicate that at least one full-time member of the security organization is onsite at all times who has the authority to direct the physical security activities of the security organization in meeting the postulated threat and is identified by position title. This individual should not have routine assignments, such as manning the CAS, SAS, etc., and must have time to direct all activities of the security organization during an incident.

guideline · An acceptable security plan would typically stipulate that the member of the security organization with authority to direct the security organization coordinates with the individual (plant manager, his designated alternate, shift supervisor, etc.) who has final responsibility for plant operation on a shift.

guideline · An acceptable security plan would typically describe a clear chain of succession of responsibility for the transfer of authority in the event of disablement of a key member of the physical security organization during an incident. This chain of succession should be described through all levels of the security organization.

§73.55(b)(3) · As part of the management system, the security plan shall describe written security procedures that document the structure of the security organization and that detail the

duties of guards, watchmen and other individuals responsible for security.

§73.55(b)(3) · As part of the management system, the security plan shall describe provisions for written approval of procedures and revisions by the individual with overall responsibility for the security function.

3.3 Qualifications for Employment in Security

§73.55(b)(4) · The security plan shall confirm that an individual does not act as a guard, watchman, armed response person, or other member of the security organization unless such individual has been trained, equipped, and qualified to perform each assigned security job duty in accordance with 10 CFR Part 73, Appendix B, "General Criteria for Security Personnel." Note: R.G. 5.20, "Training, Equipping, and Qualifying of Guards and Watchmen," has been superceded by Appendix B and should not be referenced in the plan. NUREG's 0219, 0576, and 0674 contain additional guidance concerning this bullet.

§73.55(b)(4) · The security plan shall confirm that security force personnel are trained and qualified prior to issuance of an operating license in accordance with a Commission approved training and qualification plan.

§73.55(b)(4) · The security plan shall confirm that security force personnel are requalified at least every 12 months in the applicable physical and training requirements identified in 10 CFR Part 73, Appendix B, and an approved training and qualification plan.

§73.55(b)(1)(ii)(4) · The security plan shall confirm that all results of suitability, physical and mental qualifications data and test results for security force personnel are documented and made available for NRC inspection.

§73.55(b)(4) · The security plan shall confirm that provisions have been made to demonstrate the ability of physical security personnel to carry out their assigned duties and responsibilities at the request of an authorized representative of the Commission.

3.4 Training of Plant Personnel

The following guidelines should be taken into consideration when describing security training given to nonsecurity force personnel:

guideline · An acceptable security program would typically include a training program for all nonsecurity force personnel authorized unescorted access to the protected area to assure that these individuals understand their role in physical

security and their responsibility in the event of security incidents.

guideline · An acceptable security plan would typically describe a training program that treats the threat of sabotage and is responsive to deterring, detecting and neutralizing the threat.

guideline · An acceptable security program would typically maintain documentation of completed employee training.

guideline · An acceptable security program would typically affirm to perform refresher training for such personnel to update security training.

3.5 Local Law Enforcement Liaison

§73.55(h)(2) · The security plan shall describe how liaison with local law enforcement authorities is established, documented and maintained.

guideline · An acceptable security plan would typically document the amount of response support available to the site that has been agreed upon in writing by all management of offsite response agencies. One acceptable method is the use of letters from all offsite response agencies that identify their commitment to support the facility during security incidents. The letters should state, in general terms, the level of support to be provided.

guideline · An acceptable security plan would typically describe how the written agreements of support identify and establish the following:

- the organization with the authority to direct the response onsite, (i.e., site management, specific LLEA, etc.).

- the single position of authority within the identified organization.

guideline · An acceptable security plan would typically indicate the position by title onsite at all times (if different from shift-to-shift, identify by shift) that is responsible for coordination with offsite response personnel.

guidelire · An acceptable security plan would typically address the following issues and describe the procedures to provide for:

- compatible communications with offsite response personnel.

- sufficient escorts for offsite responding personnel.

- appropriate incident management, security management, and safety interface for offsite response forces at all times.

- appropriate onsite security force interface, (while onsite).

guideline · An acceptable security program would typically, on an annual basis, provide all members of offsite response agencies with familiarization and refresher training which includes:

- plant and site tours.

- briefings on the security organization, facility personnel responsible during an incident, response procedures, and special constraints imposed on security in protecting a nuclear facility.

3.6 Security Personnel Equipment

§73.2(c) · The security plan shall confirm that all security guards wear uniforms.

guideline · An acceptable security program would typically uniform guards to be clearly distinguishable from local law enforcement and other onsite personnel.

guideline · An acceptable security plan would typically describe the manner in which other members of the security organization may be visually identified.

§73.55(b)(4) · The security plan shall confirm that members of the security force are equipped in accordance with the guidelines of 10 CFR Part 73, Appendix B.

Part 73, Appendix B · The security plan shall confirm that, as a minimum, guards and armed response individuals are armed with .38 caliber revolvers, or equivalent, and have available 12 gauge shotguns or semiautomatic rifles.

§73.55(f)(1) · The security plan shall confirm that all on-duty physical security force personnel (guards, watchmen or armed response individuals) are provided with the capability for continuous communication with the CAS/SAS.

§73.55(g)(1) · The security plan shall describe how all security personnel equipment including weapons, protective clothing, and vehicles are maintained in operable condition and shall establish an inspection, test and maintenance program for such equipment.

Part 73, Appendix B	· The security plan shall confirm that two-way two channel radios, hardwire intercom, or equivalent are used to provide the capability for continuous communication requirements for certain fixed posts, such as a defensive position or access control station.

4 PHYSICAL BARRIERS

4.1 Protected Area Barriers

§73.2(f)(1) · The security plan shall confirm that a protected area barrier is provided with penetration resistance at least equal to 11 AWG (American Wire Gauge) chain link, a top guard of barbed wire (at least three strands on brackets angled outward between 30° and 45° from the vertical), and an overall fence height of at least 8 feet.

guideline · An acceptable security plan would typically prevent undetected access to the PA by stabilizing the ground under the fence to minimize erosion of soil under the fence and by securing the bottoms of the fences in a fashion that prevents the lifting of the fence fabric.

§73.55(c)(2) · The security plan shall describe the extent to which the physical barriers at the perimeter of the protected area are separated from any other barrier designated as a physical barrier for a vital area/island within the protected area.

guideline · An acceptable security plan would typically identify any area where the PA barrier is not separated from a vital area/island barrier. Alternate physical security measures should be identified for such cases.

§73.2(f)(2) · The security plan shall confirm that the sides of buildings or walls which constitute part of the protected area barrier are at least 8 feet in height including a barbed wire topping as described above.

guideline · For buildings and walls which constitute part of the protected area barrier, an acceptable security plan would typically affirm that the buildings and walls have non-scalable facades, 18 feet or more in height. Such buildings and walls need not be protected by a top guard.

guideline · An acceptable security plan would typically assure that penetration resistance equal to that of the overall protected area barrier is provided for any culverts, ditches and other man-sized penetrations through or under the protected area barrier. Man-sized is defined as of size equal to or greater than 96 square inches with at least one dimension equal to or greater than 6 inches.

§73.55(c)(3) · The security plan shall confirm that isolation zones are maintained in outdoor areas adjacent to the physical barrier at the perimeter of the protected area. These zones should be of sufficient size to permit observation of the activities

of people on either side of that barrier in the event of its penetration.

guideline · An acceptable security program would typically extend isolation zones at least 20 feet on either side of the protected area barrier.

§73.55(c)(3) · The security plan shall confirm that employee and visitor parking facilities are located outside of isolation zones and exterior to the protected area barrier.

guideline · An acceptable security plan would typically describe the facility layout with drawing and text that affirm the existence of the PA physical barrier, the PA isolation zone, and location of parking lots beyond isolation zones.

§73.55(g)(1) · The security plan shall describe the compensatory measures used should there be a reduction in the effectiveness of a physical barrier.

guideline · An acceptable security program would typically include the following compensatory measures:

- posting of security force members with communications at the affected area to provide surveillance.
- replacement of affected barrier section(s) with spare barrier sections stored onsite.
- additional detection and alarm systems available for rapid installation.
- dedicated CCTV surveillance with dedicated monitor and observer (continuous monitoring period should not exceed 2 hrs).

guideline · An acceptable security program would typically assure that compensatory measures are of limited duration only.

§73.55(c)(4) · The security plan shall confirm that adequate response by the security organization can be initiated upon detection of penetration or attempted penetration of the protected area or the isolation zone adjacent to the protected area barrier.

§73.55(c)(4) · The security plan shall confirm that all exterior areas within the protected area are checked to detect the presence of unauthorized persons, vehicles, or materials.

guideline · An acceptable security plan would typically describe how the licensee will check the areas described in the above bullet. Such checks should be performed at random intervals and on random paths not less frequently than once every four(4) hours.

§73.55(c)(5) · The security plan shall confirm that isolation zones and all exterior areas within the protected area are provided with illumination sufficient for the monitoring and observation requirements of §73.55(c)(3), (c)(4), and (h)(4), but no less than 0.2 footcandle measured horizontally at ground level.

4.2 Vital Area/Island Barriers

§73.55(c)(1) · The security plan shall confirm that vital equipment is located only within a vital area/island which in turn is located within a protected area such that access to vital equipment requires passage through at least two physical barriers of sufficient strength to meet the performance requirements of §73.55(a). More than one vital area/island may be located within a protected area.

guideline · An acceptable security plan would typically ensure that all openings in the vital area/island barrier, especially those larger than man-sized (i.e., 96 square inches with at least one dimension equal to or greater than 6 inches) are protected so that the integrity of the barrier is not decreased.

§73.55(c)(6) · The security plan shall confirm that the walls, doors, ceiling, floors, and any windows in the walls and in the doors of the reactor control room are bullet-resisting and describe how they will be made bullet-resisting.

guideline · An acceptable security plan would typically define bullet-resisting as capable of resisting a high power rifle round (level 4) as defined in UL 752.

§73.55(d)(7) · The security plan shall describe how all points of personnel and vehicle access into vital area/islands are positively controlled.

§73.55(e)(1) · The security plan shall confirm that the onsite central alarm station is designated a vital area/island, make bullet-resisting its walls, doors, ceilings, floor, and any windows in the walls and doors and describe how they will be made bullet-resisting.

§73.55(d)(7)(v)* · The security plan shall confirm that all unoccupied vital areas/islands, not otherwise controlled, are locked and protected by an active intrusion alarm system.

guideline · An acceptable definition of the term "unoccupied vital area/island" is an area or island in which an individual can not control access to the area/island and/or cannot provide continuous surveillance over the entire area/island.

§73.55(d)(8) · The security plan shall confirm that all doors and/or hatches leading to the reactor containment are provided with locks of substantial construction to offer penetration resistance and impede both surreptitious and forced entry.

4.3 Security Posts and Structures

§73.2(s) · The security plan shall confirm that structures considered as defensive positions are bullet-resisting.

guideline · An acceptable security program would typically lock all entrance points to defensive positions at all times.

guideline · An acceptable security plan would typically affirm that defensive positions, gun ports, pass throughs, etc. are designed such that they meet the UL 752 High Power Rifle Rating and gun ports, pass throughs etc. cannot be opened from outside the defensive position nor provide access to the defensive position.

guideline · An acceptable security plan would typically describe all physical structures in the protected area credited as defensive positions for response forces and ensure that they have full fields of fire including the fence line in assigned response areas.

guideline · An acceptable security plan would typically, in addition to the CAS/SAS alarm annunciators, ensure that audible and visible intrusion alarm indication are provided within PA defensive positions for the specific alarms within that position's response area.

§73.55(f)(1) · The security plan shall describe how all guards on duty in vital areas/islands are provided with the capability of continuous communication to the central and secondary alarm stations.

4.4 Keys, Locks, and Combinations

§73.55(d)(9)* · The security plan shall describe how all security keys, locks, combinations and related equipment used to control access to the protected area and vital areas/islands are controlled to reduce the probability of compromise.

guideline R.G. 5.12 · An acceptable security plan would typically describe how the criteria of 10 CFR Part 73.2(m) and R.G. 5.12 are satisfied for all security locks, keys, combinations and related equipment.

guideline · An acceptable security program would typically distribute combinations, access cards, and keys for locks or padlocks used to secure gates or doors into protected and vital areas/islands, and for access to vital equipment, only to

those individuals authorized access to the areas in accordance with 10 CFR §73.55.

§73.55(d)(9)* · The security plan shall describe how combinations, keys, and locks used to control access to protected areas and vital areas/islands are changed whenever an individual's access authorization is revoked due to his or her lack of trustworthiness, reliability or inadequate work performance, or whenever there is evidence or suspicion that the combination or key and lock may have been compromised.

guideline · An acceptable security plan would typically affirm that keys and locks to which an employee had access be changed within 5 days, and immediately for card keys, after the employee is terminated for the reasons described above.

§73.55(d)(9)* · The security plan shall confirm that all locks, keys and combinations used to control access to protected areas and vital islands are rotated or changed at least once every 12 months.

guideline · An acceptable security plan would typically document that a record of the combinations of locks is stored in a location to which access is strictly controlled.

guideline · An acceptable security program would typically not allow keys or access cards in use to leave the protected area. These items should be accounted for at the end of each shift or workday.

guideline · An acceptable security plan would typically document the maintenance of a log listing keys and access cards, users, in and out times, and other pertinent information.

guideline · An acceptable security plan would typically, with a master system, affirm to conduct a complete remastering of the system whenever a core key, master key or change key, or a lock is lost or compromised. (Note: The use of a master key system is not recommended.)

guideline · An acceptable security program would typically affirm that a record of all locks, cores, keys and cards which might be used to compromise the integrity of the security system is stored in a location secured by a combination lock or in a secured location.

guideline · An acceptable security program would typically conduct a physical inventory of locks, cores, keys and cards used for protection of facilities once every 12 months.

guideline · An acceptable security plan would typically affirm to store unused locks, cores, keys, cards, and related equipment in a location secured by a combination lock, or in a secure location.

guideline · An acceptable security plan would typically name by position title a specific individual at each site to be placed in charge of all locks, keys, and cards.

4.5 Testing and Maintenance

§73.55(g)(1) · The security plan shall describe how all physical barriers in the PA are maintained in operable condition through an established testing and maintenance program.

§73.55(g)(1) · The security plan shall describe a testing and maintenance program established to ensure that all vital areas/islands physical barriers are maintained in operable condition.

5 ACCESS REQUIREMENTS

5.1 Access Authorizations

5.1.1 Protected Area Access

§73.55(d)(1) · The security plan shall describe how authorization for all personnel and vehicles requiring access to the PA are reviewed and checked prior to granting access to the protected area.

guideline · An acceptable security plan would typically affirm to update the list of authorization for unescorted access to the protected area at least every 31 days.

guideline · An acceptable security plan would typically document the criteria to be applied in establishing the need for access.

guideline · An acceptable security plan would typically describe the establishment and use of identification and authorization criteria for accepting packages and material for delivery into the protected area.

guideline · An acceptable security plan would typically affirm to check that packages and other materials for delivery into the protected area are expected.

guideline · An acceptable security plan would typically affirm to search all packages prior to their entry into the protected area in accordance with the criteria of Sect. 5.3 of this NUREG.

5.1.2 Vital Area/Island Access

(Note: Guidelines will be provided upon finalization of the rule requirements.)

§73.55(d)(7)* · The security plan shall describe an access authorization system that is established to limit unescorted access to vital areas/islands during nonemergency conditions to individuals who require access in order to perform their duties.

§73.55(d)(7)* · The security plan shall describe how the vital area/island access authorization system is designed to accommodate the potential need for rapid ingress or egress of individuals during emergency conditions or situations that could lead to emergency conditions.

§73.55(d)(7)(i)* · The security plan shall confirm that current authorized access lists for each vital area/island are established. These access lists should be updated and reapproved by the cognizant licensee manager or supervisor at least every

31 days. Only individuals whose specific duties require access to a vital area/island during nonemergency conditions should be included on the access list.

§73.55(d)(7)(ii)* · The security plan shall describe how all points of personnel and vehicle access to vital areas/islands are positively controlled in accordance with the access lists established pursuant to §73.55(d)(7)(i).*

§73.55(d)(7)(iii)* · The security plan shall describe how vital area/island access is controlled, during nonemergency conditions, to prevent the access of more than a single authorized person, at a time, with a single identification badge or entry device.

§73.55(d)(7)(iv)* · The security plan shall confirm that in the case of an individual's involuntary termination for cause, the individual's access authorization is revoked and his/her identification badge and other entry devices are retrieved, as applicable, prior to notifying this individual of his/her termination.

5.2 Picture Badge Systems

§73.55(d)(5) · The security plan shall describe the numbered picture badge identification system provided for all individuals who are authorized unescorted access to the protected area.

guideline · An acceptable security plan would typically affirm to visually indicate on the badge the access authorization level, PA or PA and VA. Separate vital area/island access authorization levels do not have to be visually indicated on the face of the badge but may be electronically, magnetically, etc. encoded on the badge.

§73.55(d)(5) · The security plan shall confirm that unescorted access to PAs and VAs is authorized to an individual not employed by the licensee but who requires frequent and extended access to these areas provided he receives a numbered picture badge upon entrance into the protected area which indicates (1) nonemployee, no escort required, (2) areas to which unescorted access is authorized, and (3) the period for which such access is authorized.

guideline · An acceptable security badge would typically not have to visually indicate items 2 and 3 of the bullet above, but may have these items electronically; magnetically, etc. encoded with the badge.

§73.55(d)(5) · The security plan shall commit to prohibit badges from leaving the protected area unless adequate safeguards are provided to assure that the security of the badge is not jeopardized. (Special circumstances which require a badge to be removed from the protected area should be described in the plan.)

guideline · An acceptable security plan should typically define the term: "frequent and extended."

§73.55(d)(6) · The security plan shall confirm that individuals not authorized to have unescorted access to the protected area are badged to indicate that escort is required. In addition, require such individuals to register name, date, time, purpose of visit and employment affiliation, citizenship and name of the individual to be visited.

guideline · An acceptable security program would typically provide badges for visitors and escorted individuals that are readily distinguishable and identifiable, (e.g., clearly labeled "visitor, escort required," specially colored, unique shape, etc).

§73.55(d)(5) · The security plan shall confirm that personnel are required to display badges while inside the protected area perimeter.

guideline · An acceptable security program would typically instruct employees to wear badges on the upper front portion of the body to be clearly visible except when operational or health physics reasons dictate otherwise. (In this case, the badges should be under the control of an authorized individual to assure they are not lost or misused).

5.3 Searches

5.3.1 Personnel

(Note: Guidelines will be provided upon finalization of the rule requirements.)

§73.55(d)(1)* · The security plan shall confirm that 20% (selected randomly such that it is not possible to know in advance who will be subjected to the search) of screened individuals are equipment searched (metal and explosives detectors). (Note: Screened individuals are those who possess an unescorted access authorization as provided in the proposed 10 CFR 73.56.)

§73.55(d)(1)* · The security plan shall confirm that 100% of unscreened individuals are equipment searched. (Note: Unscreened individuals are those who do not possess an unescorted access authorization as provided in the proposed 10 CFR §73.56. Individuals granted temporary access authorization during major outages as provided in 10 CFR 73.56(e)(3)* are considered unscreened.)

§73.55(d)(1)* · The security plan shall confirm that if detection equipment fails or is not in place, 20% (selected randomly such that it is not possible to know in advance who will be subjected to the search) of screened individuals, and 100% of all unscreened individuals are pat-down searched.

§73.55(d)(1)* · The security plan shall confirm that any person is pat-down searched where cause to suspect exists.

5.3.2 Vehicles

§73.55(d)(4) · The security plan shall describe how all vehicles, (except under emergency conditions or scheduled drills), are searched for items which could be used for sabotage purposes prior to entry into the protected area. Vehicle areas to be searched should include the cab, engine compartment, undercarriage, and cargo area.

§73.55(d)(4) · The security plan shall confirm that designated vehicles are limited in their use to onsite plant functions and remain in the protected area except for operational, maintenance, repair, security, and emergency purposes. (Note: See glossary for definition of designated vehicle.)

§73.55(d)(4) · The security plan shall describe how positive control is exercised over all designated vehicles to assure that they are used only by authorized persons and for authorized purposes.

guideline · An acceptable security plan would typically describe access control procedures for actual or prearranged emergency drills such that adequate control over emergency responding vehicles and personnel is maintained.

guideline · An acceptable security plan would typically affirm to search vehicles for weapons, explosives, incendiary devices, and personnel as described in previous access guidelines.

guideline · An acceptable security plan would typically search in the manner described above designated and nondesignated vehicles that leave the PA unless the vehicle and driver remain within the owner-controlled area under the observation of a member of the security force or is continually escorted by two screened individuals to ensure that the vehicle is not used to transport weapons, explosives or incendiary devices into the protected area.

5.3.3 Packages and Material

§73.55(d)(2) · The security plan shall describe how handcarried packages and material are physically searched prior to their entry into the protected area. Items should be searched for firearms, explosives, incendiary devices or other items which could be used for radiological sabotage.

§73.55(d)(3) · The security plan shall describe how all packages and material for delivery into the PA are checked for proper identification and authorization, and searched for firearms, explosives, and incendiary devices or other items that

could be used for radiological sabotage prior to admittance to the PA.

§73.55(d)(3) · The security plan shall confirm that those Commission approved delivery and inspection activities specifically designated by the licensee to be carried out within vital areas/islands or protected areas for reasons of safety, security, or operational necessity are exempted from search requirements.

§73.55(d)(2)* · The security plan shall confirm that all items carried by individuals are searched in accordance with §73.55(d)(1). When the licensee has cause to suspect that an individual is attempting to smuggle contraband articles (which could be used for radiological sabotage) within handcarried items, the licensee should physically search all handcarried items in the possession of that individual.

guideline · An acceptable security plan would typically affirm to physically search and machine search packages and material as described below:

CATEGORY I - Packages and material for other consignees on common carrier vehicles are permitted into the protected area without search provided:

1) the vehicle is escorted by a guard while within the protected area, and

2) the package and material is under the observation of a guard, and

3) the package and materials not searched are not unloaded in the protected area.

CATEGORY II - Bulk products being unloaded while under the observation of a guard constitutes an adequate search.

CATEGORY III - Packages and material excluded from search because the search could constitute a danger to the individual performing the search or would render the object being searched unusable or contaminated. Those packages and material shall be positively controlled. (For example, stored in a locked area controlled by person(s) familiar with the material.) Products for human consumption shall be positively controlled only to the extent practical. (For example, limiting lunch items to the lunch room.)

CATEGORY IV - Packages and material sealed in the manufacturing process are permitted into the protected area without search but shall be stored in locked areas and opened at their final destination point under the supervision of persons familiar with their content.

5.3.4 Search Equipment

guideline R.G. 5.7 · An acceptable security plan would typically identify the type of special detectors used for package, material, and personnel search.

guideline · An acceptable security plan would typically affirm that all search equipment is locally annunciating.

guideline · An acceptable security program would typically alarm all stationary or fixed portal search equipment to detect tampering or unauthorized access to sensitivity and calibration controls.

guideline · An acceptable security plan would typically affirm to annunciate alarms from stationary or fixed portal search equipment in the last access control point prior to PA entry in addition to locally.

guideline · An acceptable security plan would typically describe an annual performance test program for special purpose detectors.

§73.55(g)(1) · A security plan shall describe how special purpose detectors will be maintained in operable condition and how tests for operability will be conducted.

guideline · An acceptable security plan would typically affirm that an operability test will be performed on each special detector at the beginning of each shift.

5.4 Access/Entry

5.4.1 Personnel

§73.55(d)(1) · The security plan shall describe how all points of personnel and vehicle access into a protected area are controlled.

guideline · An acceptable security plan would typically ensure that personnel access to the protected area is through a lockable portal.

§73.55(d)(1) · The security plan shall describe how access authorization for all personnel and vehicles entering the PA is checked.

guideline · The security plan shall confirm that the individual controlling last access to the protected area is isolated within a bullet-resisting structure as described in §73.55(c)(6).

guideline · An acceptable security plan would typically affirm to use UL 752, High Power Rifle Rating as a standard reference for providing a bullet-resisting structure.

guideline · An acceptable security plan would typically ensure that the individual within the bullet-resisting structure controlling access to the protected area has direct observation of the portal being controlled.

guideline · An acceptable security plan would typically affirm to station two security force members at protected area personnel access portals when open: one in the bullet-resisting structure to control access, and the other to monitor and conduct searches.

guideline NUREG/CR 0510 · An acceptable security plan would typically affirm to provide duress alarms in search areas and bullet-resisting structures and annunciate them in the CAS and SAS.

guideline · An acceptable security plan would typically affirm to alarm doors providing final personnel access to the protected area and annunciate these alarms in the CAS and SAS. Portals need not be alarmed if the area is continuously manned.

guideline · An acceptable security plan would typically affirm to, in cases where the personnel access building is unoccupied, in addition to alarming the door providing access to the protected area, alarm those portions of the building making up the protected area barrier.

guideline · An acceptable security plan would typically ensure that all admittance control hardware other than special purpose detectors clearly annunciate warnings at the portal and within the bullet-resisting structure from which access is controlled.

§73.55(f)(1),(3) · The security plan shall describe how posted guards or watchmen are provided with the capability of continuous communication from the protected area portal to the CAS and SAS.

5.4.2 Vehicles

guideline · An acceptable security plan would typically ensure that vehicle access to the protected area is through a gate which is locked and controlled by a member of the security force from within a bullet-resisting structure. Vehicle access control should be maintained by two members of the security force with continuous communications capability to the CAS and SAS at the portal during the time of vehicle access. The communications capability should be provided by two-way radio, hardwire intercom, or plant telephone system.

guideline · An acceptable security plan would typically define the term "designated vehicle" as a vehicle authorized unescorted access to the protected area by work order or equivalent

written permission for a work-related need, operated by an individual granted unescorted access and searched in accordance with Section 5.3.2.

§73.55(d)(4) · The security plan shall confirm that designated vehicles are limited in their use to onsite plant functions and ensure they remain in the protected area except for operational, maintenance, repair, security, and emergency purposes.

guideline · An acceptable security plan would typically define the term "nondesignated vehicle" as a vehicle granted PA access by work orders or equivalent written permission for work-related need, operated by individuals not granted unescorted access and searched in accordance with Section 5.3.2. These vehicles require escort by 2 members of the security organization.

guideline · An acceptable security plan would typically affirm to lock the ignition, remove the keys from the ignition and place the keys in the custody of the escort when nondesignated vehicles are unattended.

5.5 Escorts

§73.55(d)(6) · The security plan shall describe how individuals not authorized by the licensee to enter protected areas without escort are escorted by a watchman or other designated individual while within the protected area.

guideline · An acceptable security plan would typically affirm that escorts are provided for unauthorized individuals throughout the protected area including all vital areas/islands within the protected area.

§73.55(d)(6) · The security plan shall describe how individuals requiring escorts are badged to indicate that an escort is required.

§73.55(d)(6) · The security plan shall confirm that an escorted individual is required to register: name, date, time, purpose of visit, employment affiliation, citizenship, and name of the individual to be visited.

guideline · An acceptable security plan would typically affirm to determine the ratio of escorts to visitors requiring escorts depending upon the ability of the escort to provide direct observation of the activities of the group. A nominal visitor to escort ratio within the protected area is 10:1, within a vital area/island, 5:1. Licensee training, classroom, and meeting situations may exceed the 10:1 ratio.

guideline · An acceptable security plan would typically ensure that escorts are individuals authorized unescorted access to protected areas and vital areas/islands and have been trained in their escort duties.

§73.55(d)(4) · The security plan shall describe how all vehicles, except designated vehicles, requiring entry into the PA are escorted by a member of the security organization while within the PA and to the extent practicable off-loaded in the protected area at a specific designated materials receiving area that is not adjacent to a vital area/island.

guideline · An acceptable security plan would typically describe how escorts for nondesignated vehicles are provided with communications to the CAS and SAS while within vital areas/islands.

5.6 Vital Area/Island Compartmentalization

Note: Effective guidelines will be provided upon finalization of the rule requirements.)

guideline* · An acceptable security program would typically categorize vital areas as Type I or Type II vital areas for the purpose of vital island designation. Type I vital areas are single vital areas wherein radiological sabotage can be accomplished. Type II vital areas are those wherein radiological sabotage can be accomplished only in conjunction with additional sabotage activity in at least one other separate vital area. All type I vital areas should be protected within a vital island.

guideline* · An acceptable security program would typically locate at least one Type II vital area of each complete set of Type II vital areas in one or more protected vital islands.

§73.2(nn)* · The security plan shall confirm that "vital islands" are designated as combinations of vital areas such that radiological sabotage exceeding 10 CFR Part 100 release criteria cannot be accomplished without entry into at least one vital island.

§73.55(c)(1)* · The security plan shall confirm that for access to vital areas/islands, passage through at least two physical barriers of sufficient strength to meet the performance requirements of §73.55(a) is required.

§73.55(d)(7)* · The security plan shall describe that an access authorization system, established to limit unescorted access to vital areas/islands during nonemergency conditions to individuals who require access in order to perform their duties.

guideline* · An acceptable security program would typically design an access authorization system to accommodate the potential need for rapid ingress or egress of individuals during emergency conditions or situations that could lead to emergency conditions.

§73.55(d)(7)(i)* · The security plan shall describe how current authorized access lists are established and maintained for each vital area/island. These access lists should be updated and reapproved by the cognizant licensee manager or supervisor at least every 31 days. Only individuals whose specific duties require access to a vital island during nonemergency conditions should be included on the access lists.

§73.55(d)(7)(ii)* · The security plan shall describe how all points of personnel and vehicle access to vital areas/islands are positively controlled.

§73.55(d)(7)(iii)* · The security plan describe how vital area/island access controls are used during nonemergency conditions to prevent the access of more than a single authorized person at a time with a single identification badge or entry device.

§73.55(d)(7)(iv)* · The security plan shall confirm that in the case of an individual's involuntary termination for cause, the individual's access authorization is revoked and his/her identification badge and other entry devices, as applicable, are retrieved prior to notifying this individual of his/her termination.

§73.55(d)(7)(v)* · The security plan shall confirm that unoccupied vital areas/islands and all exterior doors leading to vital areas/islands which are not otherwise controlled are locked and protected by an active intrusion alarm.

§73.55(e)(1)* · The security plan shall confirm that all onsite emergency power supply systems for alarm annunciator equipment and nonportable communications equipment are located within vital areas/islands.

§73.55(d)(8) · The security plan shall describe how any time frequent access is permitted to containment, such as during refueling or major maintenance, the access is tightly controlled to assure that only authorized personnel and material are permitted into the containment. Such control should be exercised by the licensee through the use of guard or watchman.

guideline · An acceptable security plan would typically affirm that reactor containment will not be de-vitalized.

5.7 Records

§73.70(a) · The security plan shall confirm that a record of the names and addresses of all individuals who have been designated as authorized individuals is maintained.

guideline · An acceptable security plan would typically affirm to maintain the record described in the bullet above for the length of employment plus one year.

§73.55(b)(4)	• A security plan shall describe how security force annual requalification training is accomplished and maintained.
guideline NUREG's 0219, 0576, 0674	• An acceptable security plan would typically affirm to maintain individual security training records for a period of one year.
guideline	• An acceptable security plan would typically affirm to maintain records of an individual's access to locks, keys, combinations, and other related equipment for the period of employment or for the duration that such locks, keys, and combinations are used.
§73.70(e)	• The security plan shall describe a system for documenting all security tours and inspections, and all tests, inspections and maintenance performed on physical barriers, intrusion alarms, communications equipment and other security-related equipment.
guideline	• An acceptable security plan would typically affirm to maintain such documentation for a period of 12 months.
guideline	• An acceptable security program would typically establish and maintain procedures for controlling access to protected areas and for controlling access to keys for locks used to protect special nuclear material.
§73.70(b)	• The security plan shall confirm that a record of all persons authorized access to vital equipment and areas is established and maintained.
guideline	• An acceptable security plan would typically affirm to maintain the record described in the bullet above for the length of employment plus one year.
§73.70(d)*	• The security plan shall confirm that a log indicating the name, badge number, time of entry, reason for entry and time of exit of all individuals granted access to a vital area/island is established and maintained.
§73.70(c)*	• The security plan shall confirm that a register of visitors, vendors, and other individuals not employed by the licensee pursuant to §73.55(d)(6) is established and maintained.
guideline	• An acceptable security plan would typically affirm to maintain the register described in the bullet above for a period of 1 year.

6 DETECTION AIDS

6.1 Illumination

§73.55(c)(5) · The security plan shall describe how illumination of isolation zones and all exterior areas within the protected area is maintained sufficient for the monitoring and observation requirements of §73.55(c)(3), (c)(4), and (h)(4) but no less than 0.2 foot candles measured horizontally at ground level.

guideline · An acceptable security plan would typically affirm to maintain illumination of the tops and sides of all accessible structures. Note: A structure should be considered "accessible" if it is less than 18 feet in height or has a ready means of access to the roof, such as ladders, stairs, climbing bars, etc.

§73.55(c)(5) · The security plan shall describe how isolation zones and all exterior areas within the PA are maintained at a minimum level of illumination of 0.2 foot candles measured horizontally at ground level.

guideline · An acceptable security plan would typically identify compensatory measures for the security lighting system. Acceptable compensatory measures for failure or degradation of the lighting system include:
- installation of portable lighting equipment.
- rendering shadowed areas unfit for cover.
- positioning of security personnel at strategic locations.
- use of low light level surveillance equipment.

guideline · An acceptable security plan would typically identify areas that could conceal a man and compensatory measures to allow for surveillance of the areas.

guideline · An acceptable security plan would typically affirm that sufficient illumination is provided to allow use of CCTV systems.

6.2 Surveillance

§73.55(h)(6) · The security plan shall describe how the capability of observing the isolation zones and the physical barrier at the perimeter of the protected area is provided, preferably by means of closed circuit television or by other suitable means which limit exposure of response personnel to possible attack. The purpose of this capability is to facilitate initial response to detection of penetration of the PA and the assessment of the existence of a threat.

guideline · An acceptable security plan would typically affirm that the fixed CCTV system includes a field of view for the entire isolation zones (both sides of the PA barrier) as specified in §73.55(h)(6).

guideline · An acceptable security program would typically locate CCTV cameras within the field of view of other cameras used for isolation zone and protected area barrier surveillance.

guideline · An acceptable security program would typically provide the CAS and SAS with sufficient monitoring devices and controls to adequately use and manage the CCTV system.

guideline · An acceptable security plan would typically identify any areas where CCTV surveillance/assessment is not possible and those measures used to provide equivalent surveillance/assessment capabilities of the areas.

guideline · An acceptable security program, if surveillance/assessment is provided by guards, would typically locate guard positions within the field of view of other guards or CCTV.

§73.55(g)(1) · The security plan shall identify and describe the measures used to compensate for loss of the surveillance/assessment system or portions of the system.

guideline · An acceptable security program would typically transmit equivalent surveillance data to the central and secondary alarm stations for simultaneous monitoring.

guideline · An acceptable security plan would typically assure, if CCTV surveillance is used as a compensatory measure to monitor a malfunctioning zone or alarm point, that the monitor is manned by a member of the security force, (other than the CAS and SAS operator), dedicated to that function. Personnel should not perform this function for a continuous period of time exceeding 2 hours.

6.3 Alarm/Intrusion

§73.55(c)(4) · The security plan shall describe how detection of penetration or attempted penetration of the protected area or the isolation zone adjacent to the protected area barrier will assure that adequate response by the security organization can be initiated.

guideline · An acceptable security plan would typically affirm that building walls making up part of the PA barrier are provided with an intrusion detection system along the front or top of the wall constituting the PA barrier.

guideline NUREG 320 · An acceptable security program would typically ensure that for each zone the PA intrusion detection system is capable of detecting 95 cut of 100 intrusions by running, walking,

crawling, rolling, or jumping intruders as stated in R.G. 5.44.

guideline NUREG/CR 0509

- An acceptable security program would typically include the following emergency power for intrusion detection systems:

  - an automatic switchover from primary power to a uninterruptible power source, e.g., emergency battery and generator or emergency battery power, without causing an alarm, but with indication in the CAS and SAS.

  - capability of twenty-four (24) hours of operation without recharging batteries or refueling generators unless charging capabilities or fuel is located on site.

§73.55(e)(1)

- The security plan confirm that all alarms required pursuant to 10 CFR Part 73 annunciate in a continuously manned central alarm station located within the protected area and in at least one other continously manned station not necessarily onsite such that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm.

guideline NUREG-0320

- An acceptable security program would typically provide an audible and visual indication of alarm conditions for all intrusion detections.

§73.55(e)(2)

- The security plan shall confirm that the type and location/zone or alarm point of all incoming alarms are identified through the alarm annunciation system.

§73.55(e)(2)

- The security plan shall confirm that power failure and indication that the system is on stand-by power are annunciated.

guideline

- An acceptable security program would typically annunciate the following alarm conditions:

  - intrusion
  - tamper/line supervision
  - power failure & indication of switchover to emergency power
  - other alarm conditions appropriate to the system.

§73.55(d)(7)

- The security plan shall describe how unoccupied vital areas/islands are protected by active intrusion alarm systems.

§73.55(d)(8)

- The security plan shall describe how doors and/or hatches for access to the reactor containment are alarmed.

§73.55(e)(3) · The security plan shall describe how all emergency exits in each protected area and each vital area/island are alarmed.

6.4 False and Nuisance Alarm Rates

guideline · An acceptable security plan would typically ensure that the frequency of false or nuisance alarms for all intrusion alarm systems does not degrade the response capability.

6.5 Tamper Indication and Self-Test Capabilities

§73.55(e)(2) · The security plan shall confirm that all intrusion detection systems are tamper indicating and self-checking, (e.g., an automatic indication is provided when failure of an alarm system or a component occurs, or when the system is on standby power).

guideline · An acceptable security program would typically use the following list as acceptable means for providing tamper-indicating or self-checking capabilities:

- equip all enclosures including, but not limited to, CAS and SAS equipment cabinets, junction boxes in which wires are joined, etc. with tamper switches or trigger mechanisms compatible with the alarm system.
- ensure trigger mechanisms/tamper switches remain in operation when the system is in the ACCESS mode.
- locate controls that affect sensitivity of alarm systems within tamper-indicating enclosures.
- supervise signal lines connecting alarm relays with alarm processors and/or monitors.

guidelines NUREG 0320 · An acceptable security plan should prohibit the use of radio transmitted line supervision for the purpose of providing line supervision.

6.6 Compensatory Measures

§73.55(g)(1) · The security plan shall describe that compensatory measures are established and employed to ensure that an equivalent level of protection is provided in the event of detection hardware outages.

guidelines · An acceptable security program should affirm the following as acceptable compensatory measures:

- posting of guards or watchmen with communications to the CAS and SAS within the affected zone or at the affected alarm point to provide visual surveillance.

- deployment of back-up intrusion detection hardware to the affected zone or alarm point.

- use of CCTV surveillance of the affected zone or alarm point by a member of the security force other than the CAS and SAS operator, dedicated to monitoring the CCTV monitor. Personnel should not provide such a monitoring function for a continuous period exceeding 2 hours.

6.7 Central Alarm Station/Secondary Alarm Station Operation

§73.55(e)(1) · The security plan shall identify the onsite central alarm station as a vital area/island.

§73.55(e)(1) · The security plan shall describe that the central alarm station is located within a building such that the interior of the station is not visible from the perimeter of the protected area.

§73.55(e)(1) · The security plan shall describe that any operational activities interfering with the execution of the alarm response function are not contained within the central alarm station.

§73.55(e)(1) · The security plan shall describe the walls, doors, ceiling, floor and any windows in the walls and doors of the central alarm station as bullet-resisting.

guidelines NUREG/CR-0543 · An acceptable security plan would typically affirm to use UL 752, High Power Rifle Rating as a standard such that personnel and essential communications equipment within the CAS are provided protection against bullet penetration.

guidelines NUREG/CR-0543 · An acceptable security program would typically make the SAS bullet-resistant if it is the last access control point to the PA or VA.

guidelines NUREG/CR-0543 · An acceptable security plan would typically affirm to lock at all times all portals (windows, doors, etc.) which would permit personnel entry, (aperture area exceeding 96 square inches with one dimension equal to or exceeding six inches) to the central alarm station or secondary alarm station.

guidelines · An acceptable security program would typically affirm not to collocate the SAS with the control room or other high traffic open areas.

§73.55(d)(7) · The security plan shall describe that access to the central alarm station is authorized to only those personnel with an operational need or security-related duties.

§73.55(e)(1) · The security plan shall describe that all alarms required pursuant to 10 CFR Part 73 annunciate in a continuously manned central alarm station located within the protected area and in at least one other continously manned alarm station not necessarily onsite such that a single act cannot remove the capability of calling for assistance or responding to an alarm.

guidelines · An acceptable security program would typically annunciate all alarms within one second of activation at the continually manned alarm stations in such a manner that the operator is aware of the alarm and can initiate response actions.

§73.55(e)(2) · The security plan shall describe that the central and secondary alarm stations alarm annunciations will indicate the type of alarm and its location.

guidelines · An acceptable security program would typically prohibit the central and secondary alarm station operators from changing an alarm point status or activating any locking or controlling device at protected or vital area/island portals without the knowledge of the other alarm station operator.

guidelines
NUREG-0320
NUREG/CR-0509 · An acceptable security program would typically provide the alarm stations with a source of emergency power capable of supplying power to all required security functions. Possible methods include: UPS, battery-generator systems, emergency busses, etc.

guidelines · An acceptable security plan would typically ensure that all annunciation and other alarm or surveillance system hardware, including transmission lines, junction boxes, equipment cabinets, etc. which provides direct access to cable terminations or other unsupervised alarm equipment is tamper-indicating and self-checking, e.g., an automatic indication is provided when failure of the alarm system or component occurs, or when the system is on stand-by power.

§73.55(e)(1) · The security plan shall describe that the alarm stations are continuously manned by at least one authorized individual.

guidelines · An acceptable security program should permit only members of the security organization to man alarm stations.

K73.55(f)
(1),(2),(3) · The security plan shall describe that both the central and secondary alarm stations are provided with the following capabilities.

- continuous communications with each guard, watchman, or armed response individual on duty.
- conventional telephone service with local law enforcement agencies.

- radio or microwave transmitted two-way voice communications, either directly or through an intermediary, in addition to conventional telephone service between local law enforcement agencies and the faci ity. Such communication should terminate in each continuously manned alarm station.

guidelines NUREG-0320 · An acceptable security plan would typically provide the following capabilities for both the central and secondary alarm stations:

- continous communication with fixed posts in the PA and vital areas/islands.
- continuous communication with the plant control room.
- fully independent and redundant wire and wireless communications wi.n LLEA.

guidelines · An acceptable security plan would typically affirm that the annunciator hardware is consistent with NUREG-0320.

6.8 Security Patrols

§73.55(c)(4) · The security plan shall describe that all exterior areas within the protected area are periodically checked to detect the presence of unauthorized personnel or material.

guidelines · An acceptable security plan would typically affirm to patrol the protected area perimeter barrier and adjacent isolation zones at random times and on random paths at least once every four hours.

guidelines · An acceptable security plan would typically affirm, as a minimum, to check for unauthorized individuals within the protected area, breaches in barriers, and all exterior portions within the protected area while on patrol.

§73.55(f)(1) · The security plan shall describe that patrolling individuals are provided with continuous communication with the central and secondary alarm stations.

guidelines · An acceptable security program would typically reevaluate the use of patrols if defensive positions are established, manned, and have clear fields of view of the perimeter barrier and exterior portions of the protected area.

6.9 Testing and Mai.t.nance

§73.55(g) · The security plan shall describe that intrusion alarms, emergency alarms, communications equipment, physical

barriers and other security related devices or equipment utilized pursuant to §73.55 are tested and maintained.

73.55(g)(1) · The security plan shall describe that all alarms and physical barriers are maintained in operable condition.

§73.55(g)(2) · The security plan shall describe that each intrusion alarm is 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 7 days, the intrusion alarm should be tested at least once every seven days.

6.10 Records

guidelines · An acceptable security program would typically maintain initial qualification tests of security equipment for the life of the equipment.

guidelines · An acceptable security program would typically maintain records of security equipment maintenance for a period of one year.

§73.70(f) · The security plan shall describe that a system for recording each alarm, false alarm, alarm check, and tamper indication is established and maintained that identifies: 1) date and time of alarm annunciation, 2) type of alarm, 3) location of alarm detector, 4) alarm circuit, and 5) determination as to the cause of the alarm and incident findings as determined by the responding security organization members.

7 COMMUNICATIONS

7.1 General Communications Requirements

§73.55(f)(1)

- The security plan shall describe that each guard, watchman or armed response individual on duty is capable of maintaining continuous communications with an individual in each continuously manned alarm station required by §73.55(e)(1) who should be capable of calling for assistance from other guards, watchmen and armed response personnel and from local law enforcement authorities.

§73.55(f)(2)

- The security plan shall describe that alarm stations required by §73.55(e)(1) are provided with conventional telephone service for communication with law enforcement authorities as described in §73.55(f)(1).

§73.55(f)(3)

- The security plan shall describe that in order to establish continuous communication, radio or microwave transmitted two-way voice communication is provided either directly or through an intermediary, in addition to conventional telephone service, between LLEA and the facility and terminates in each continously manned alarm station.

§73.55(f)(4)

- The security plan shall describe that all nonportable communications (e.g., radio, microwave links, etc.) are provided with an independent source of emergency power in the event of loss of normal power.

guidelines NUREG/CR-0509

- An acceptable security plan should affirm to provide all central communications equipment (e.g., telephone, intercoms, public address, etc.) which are critical to directing and controlling response forces or the security organization with an onsite source of emergency power. Acceptable sources include UPS, battery generated systems, emergency buses, etc.

guidelines

- An acceptable security plan would typically affirm the use of two distinct and independent channels (i.e., not of the same frequency such that transmission and reception constitute one channel) for communications.

guidelines

- An acceptable security plan would typically affirm that there are no areas within the protected area or reactor associated buildings where communications with the CAS and SAS is not possible. In cases where areas have been identified where use of portable radios would interfere with plant monitoring equipment, etc., affirm that an alternate means of communication with the CAS and SAS is provided.

guidelines

- An acceptable security program would typically provide tamper indication for associated amplification cabinets, telephone closets, or similar points within the PA where security communications can be disrupted.

7.2 Testing and Maintenance of Communication Systems

§73.55(g)(1)

- The security plan shall describe that communications equipment is maintained in operable condition.

§73.55(g)(3)

- The security plan shall describe that equipment required for onsite communications is performance tested not less frequently than once at the beginning of each security personnel work shift.

§73.55(g)(3)

- The security plan shall describe that equipment required for communications offsite is performance tested not less than once a day.

8 EVALUATION AND AUDIT OF PHYSICAL SECURITY AT PLANT

§73.55(g)(4) · The security plan shall describe that an annual audit program for the physical security program is established and maintained.

§73.55(g)(4) · The security plan shall describe that individuals, independent of the security organization management and supervision, performing the audit are identified.

§73.55(g)(4) · The security plan shall describe that the following is included in the audit: a review and audit of security procedures, evaluation of the effectiveness of the physical protection system, an audit of the physical protection system testing and maintenance program and an audit of communications established for response by local law enforcement authorities.

§73.55(g)(4) · The security plan shall describe that the results of the review audit and evaluation are documented along with the recommendations for corrections and improvements.

§73.55(g)(4) · The security plan shall describe that the audit report is retained and available for inspection for a period of 5 years.

§73.55(g)(4) · The security plan shall describe that results of the review are reported to plant management and to corporate management at least one level higher than that having responsibility for the day-to-day plant operation.

guidelines · An acceptable security plan would typically affirm to correct any deficiencies identified by the audit and identify the responsible organization for assuring timely correction.

9 RESPONSE CAPABILITIES

§73.55(h)(3) · The security plan shall describe that ten (10) armed responders are provided per shift and are immediately available at all times regardless of routine or emergency duties. A lesser number of armed responders, but not less than five (5), may be adequate based on an evaluation of the facility using NUREG 0907, "Acceptance Criteria for Determining Armed Response Force Size at Nuclear Power Plants."

guidelines · An acceptable security plan would typically, if the armed response force is less than ten, describe additional features of the security program to justify the reduction in the response force. These features may include:

(a) Selection, training and motivation of response force.

(b) Availability and construction of defensive positions.

(c) Availability and knowledge of weapons and other equipment.

(d) Individual site considerations, including size, topography, configuration, geography, weather, and number of nuclear power plant units.

(e) Location and reliability of initial detection devices.

(f) Consideration of local law enforcement agencies response.

(g) Vital area/island hardening, including plant design, location of and access control to vital areas/islands.

(h) Design and construction of protected area barriers.

(i) Redundancy of security systems.

(j) Initial clearance and continuing reliability assessment of personnel.

(k) Security and contingency procedures.

guidelines · An acceptable security program would typically designate the post assignments by shift necessary to implement the requirements of 10 CFR Part 73, Appendices B and C to Part 73, and commitments of the security plan.

guidelines · An acceptable security plan would typically provide a sufficient number of security force personnel for the

continuous manning of the CAS and SAS as well as other posts and duties which could not be terminated to perform the response function.

guidelines · An acceptable security program may use security force personnel for nonsecurity related duties, (e.g., fire brigade), provided the CAS and SAS are manned and a minimum number of five armed responders are immediately available for response duties.

guidelines · An acceptable security program would typically ensure that armed response force personnel do not have any operational, security or emergency duties that interfere with their ability to immediately respond to a security incident.

§73.55(c)(4) · The security plan shall describe that detection of penetration or attempted penetration of the protected area or the isolation zone adjacent to the protected area is ensured to enable adequate initiation of response by the security organization.

§73.55(h)(1) · The security plan shall describe when appropriate, the execution of a safeguards contingency plan executed for dealing with threats, thefts, and radiological sabotage related to the nuclear facilities subject to the provisions of 10 CFR 73.55. Safeguards contingency plans should be in accordance with the criteria in 10 CFR Part 73, Appendix C.

guideline R.G. 5.54 · An acceptable security plan may include the contingency plan as part of the security plan or the contingency plan may be a separate plan.

§73.55(h)(4) · The security plan shall describe that the following action is taken upon detection of abnormal presence or activity of persons or vehicles within an isolation zone, a protected area, material access area, or a vital area/island or upon evidence or indication of intrusion into a protected area, a material access area, or a vital area/island:

1) determine whether or not a threat exists

2) assess the extent of the threat, if any,

3) take immediate concurrent measures to neutralize the threat by: a) requiring responding guards or other armed response personnel to interpose themselves between vital areas/islands and material access areas and any adversary attempting entry for the purpose of radiological sabotage or theft of special nuclear material and to intercept any person exiting with special nuclear material and b) informing the local law enforcement agencies of the threat and requesting assistance.

§73.55(h)(5) · The licensee shall instruct every guard and armed response personnel to prevent or impede attempted acts of theft or radiological sabotage by using force sufficient to counter the force directed at him including the use of deadly force when the guard or other armed response person has a reasonable belief that it is necessary in self-defense or in the defense of others.

10 SPECIAL SITUATIONS AFFECTING SECURITY

guideline

- An acceptable security program would typically implement procedures for inspecting all devitalized vital areas/islands and equipment which may have been accessed during refueling/major maintenance operations.

guideline

- An acceptable security program would typically develop and maintain provisions to assure that there will be no increase in the likelihood of successful radiological sabotage during refueling or major maintenance operations.

guideline

- An acceptable security plan would typically affirm that the level of protection afforded a plant site is not diminished by construction activities at any adjacent site. Interim barriers, intrusion detection systems, guard patrols, etc. should be described in this section.

§73.55(d)(8)

- The security plan shall describe how any time frequent access any time frequent access is permitted to containment, such as during refueling or major maintenance, it is positively controlled to assure that only authorized personnel and material are permitted into the containment. (Such control should be exercised by the licensee through the use of a guard or watchman.)

guideline

- An acceptable security plan would typically affirm to prohibit the de-vitalization of reactor containment.

guideline

- An acceptable security plan would typically describe the special security measures used when two separate protected areas each containing vital areas/islands are located within one owner-controlled area, (e.g., additional response, intrusion alarms, search, access control, or lighting measures).

APPENDIX A

GLOSSARY OF SELECTED TERMS

APPENDIX A

GLOSSARY OF SELECTED TERMS

NOTE: This glossary presents staff interpretation on selected terms used in this document. The interpretations of these selected terms are not intended to supercede or replace any definitions found in 10 CFR Part 73.

1. Annual requirements: Annual requirements are defined as once every twelve (12) months, however, some variation to this time period may be acceptable depending upon documented circumstances.

2. Bullet-resisting: Bullet-resisting is defined as capable of resisting a high power rifle round (level 4) as defined in UL752.

3. Designated vehicle: A designated vehicle is a vehicle authorized unescorted access to the protected area by work order or equivalent written permission for a work-related need, operated by an individual granted unescorted access and searched in accordance with Section 5.3.2 of this document.

4. Non-designated vehicle: A non-designated vehicle is a vehicle granted PA access by work order or equivalent written permission for a work-related need, operated by individuals not granted unescorted access and searched in accordance with Section 5.3.2 of this document. These vehicles require escort by two (2) members of the security organization.

5. Unoccupied vital area/island: An unoccupied vital area/island is an area or island in which an individual cannot control access to the area/island and/or cannot provide continuous surveillance over the entire area/island.

APPENDIX B

BIBLIOGRAPHY OF SELECTED NRC DOCUMENTS

APPENDIX B

BIBLIOGRAPHY OF SELECTED NRC DOCUMENTS

REGULATORY GUIDES

R.G. 5.7	Entry/Exit Control for Protected areas, Vital Areas and Access Areas.
R.G. 5.12	General Use of Locks in the Protected and Control of Facilities and Special Nuclear Material.
R.G. 5.14	Use of Visual Surveillance Techniques in Material Access Areas.
R.G. 5.43	Plants Security Force Duties.
R.G. 5.44	Perimeter Intrusion Alarm Systems (Revision 1).
R.G. 5.XX	Standard Format and Content Guide for the Nuclear Reactor Access Authorization Rule (to be published).

NUREGS

NUREG-0178	Basic Considerations for Assembling a Closed-Circuit Television System
NUREG-0219	Nuclear Security Personnel for Power Plants
NUREG-0320	Interior Intrusion Alarm Systems
NUREG-0464	Site Security Personnel Training Manual (4 Volumes)
NUREG/CR-0484	Vehicle Access and Control Planning Document
NUREG/CR-0485	Vehicle Access and Search Training Manual
NUREG-0508	Security Communications Systems for Nuclear Fixed-Site Facilities
NUREG/CR-0509	Emergency Power Supplies for Physical Security Systems
NUREG/CR-0510	Duress Alarms for Nuclear Fixed Site Facilities
NUREG/CR-0532	Safeguards Against Insider Collusion (Volume 1)
NUREG/CR-0543	Central Alarm Station and Secondary Alarm Station Planning Document
NUREG-0576	Nuclear Power Reactor Security Personnel Training and Qualification Plan
NUREG-0674	Security Personnel Training and Qualification Criteria
NUREG-0768	People Related Problems Affecting Security in the Licensed Nuclear Industry
NUREG/CR-1327	Security Personnel Training and Qualification Criteria
NUREG/CR-1378	Hardening Existing SSNM Storage Facilities
NUREG/CR-1468	Design Concepts for Independent Central Alarm Station and Secondary Alarm Station Intrusion Detection Systems
NUREG-XXXX	Vital Area Designation and Protection (to be published)

NRC FORM 335 (7-77)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG-0908

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plans

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
Power Reactor SG Licensing Branch

5. DATE REPORT COMPLETED
MONTH: May | YEAR: 1982

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Division of Safeguards
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

DATE REPORT ISSUED
MONTH: August | YEAR: 1982

6. *(Leave blank)*

8. *(Leave blank)*

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Division of Safeguards
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

10. PROJECT/TASK/WORK UNIT NO.
02552

11. CONTRACT NO.
N/A

13. TYPE OF REPORT
Licensing Guidance

PERIOD COVERED *(Inclusive dates)*
Effective until further notice

15. SUPPLEMENTARY NOTES

14. *(Leave blank)*

16. ABSTRACT *(200 words or less)*
This guidance document contains acceptance criteria to be used in the NRC license review process. It contains specific criteria for use in evaluating the adequacy of nuclear power reactor security programs as detailed in security plans.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS
acceptance criteria
security plans
physical protection

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS *(This report)*
U

21. NO. OF PAGES

20. SECURITY CLASS *(This page)*
U

22. PRICE
$

NRC FORM 335 (7-77)

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

FOURTH CLASS MAIL
POSTAGE & FEES PAID
USNRC
WASH D C
PERMIT No G67