

JAN 18 1979

Distribution:

Docket File

NRC PDR

Local PDR

LWR #4 File

D. Vassallo

F. Williams

S. Varga

D. Lynch

M. Service

ELD

IE (3)

Miller

2. Clark

bcc:

J. Buchanan, NSIC

T. Abernathy, TIC

ACRS (16)

Docket No: 50-397

Mr. Neil O. Strand  
Washington Public Power Supply System  
300 George Washington Way  
P. O. Box 968  
Richland, Washington 99352

Dear Mr. Strand:

In reviewing your Physical Security Plan for the WNP-2 facility submitted on December 21, 1978, we find that there is insufficient information contained in your report. The lack of information is such that we cannot continue our review, including the formulation of Round 1 questions on your proposed Security Plan. The lead reviewer for your Security Plan, Mr. A. Sinisgalli, subsequently contacted J. Sorenson of your organization by telephone on January 12, 1979, to determine the reasons for these obvious deficiencies. During this telephone conversation, Mr. Sinisgalli determined that the primary cause of the weaknesses in your Physical Security Plan is that you do not have: (1) the latest revisions of the staff's guidance on the evaluation of security plans provided to the branch members of the Reactor Safeguards Licensing Branch; and (2) a copy of the staff's Security Plan evaluation Report Workbook. Accordingly, we are forwarding to you a complete and current set of the staff's Review Guidelines, including all revisions through November 6, 1978 (Attachment 1). Additionally, we are forwarding to you a copy of the workbook cited above (Attachment 2).

Upon receipt of these two attachments we recommend that you review the WNP-2 report on the Physical Security Plan and consider expanding your report in light of the guidance provided by these two attached documents. Upon completing this reevaluation of your physical Security Plan, we request that you contact M. D. Lynch (301-492-7831) to

(see non-prop  
reports)

AP3

17802060011

GD

OFFICE >						
SURNAME >						
DATE >						

Mr. Neil O. Strand

-2-

JAN 18 1979

arrange a meeting at which we can discuss any proposed revisions to your Physical Security Plan that you might be contemplating. The purpose of this proposed procedure is to expedite our review of your Security Plan. We plan to issue Round 1 questions, if appropriate, after receipt of your revised Security Plan Report.

Please contact us if you require any discussion or clarification of this matter.

Sincerely,

Original signed by:  
S. A. Varga

Steven A. Varga, Chief  
Light Water Reactors Branch No. 4  
Division of Project Management

cc: See next page  
w/enclosure  
(see reports - non-prop)

OFFICE	DPM: LWR #4	DPM: LWR #4			
SURNAME	DLynch:tlb	SVarga	RCClark		
DATE	1/17/79	1/18/79	1/17/79		



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

JAN 18 1979

Docket No: 50-397

Mr. Neil O. Strand  
Washington Public Power Supply System  
300 George Washington Way  
P. O. Box 968  
Richland, Washington 99352

Dear Mr. Strand:

In reviewing your Physical Security Plan for the WNP-2 facility submitted on December 21, 1978, we find that there is insufficient information contained in your report. The lack of information is such that we cannot continue our review, including the formulation of Round 1 questions on your proposed Security Plan. The lead reviewer for your Security Plan, Mr. A. Sinisgalli, subsequently contacted J. Sorenson of your organization by telephone on January 12, 1979, to determine the reasons for these obvious deficiencies. During this telephone conversation, Mr. Sinisgalli determined that the primary cause of the weaknesses in your Physical Security Plan is that you do not have: (1) the latest revisions of the staff's guidance on the evaluation of security plans provided to the branch members of the Reactor Safeguards Licensing Branch; and (2) a copy of the staff's Security Plan evaluation Report Workbook. Accordingly, we are forwarding to you a complete and current set of the staff's Review Guidelines, including all revisions through November 6, 1978 (Attachment 1). Additionally, we are forwarding to you a copy of the workbook cited above (Attachment 2).

Upon receipt of these two attachments we recommend that you review the WNP-2 report on the Physical Security Plan and consider expanding your report in light of the guidance provided by these two attached documents. Upon completing this reevaluation of your physical Security Plan, we request that you contact M. D. Lynch (301-492-7831) to

Docket # 50-397  
Control # 7902060011  
Date 1/18/79 of Document  
REGULATORY DOCKET FILE



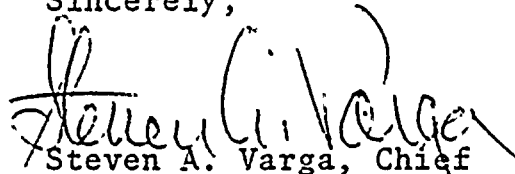
Mr. Neil O. Strand

-2-

arrange a meeting at which we can discuss any proposed revisions to your Physical Security Plan that you might be contemplating. The purpose of this proposed procedure is to expedite our review of your Security Plan. We plan to issue Round 1 questions, if appropriate, after receipt of your revised Security Plan Report.

Please contact us if you require any discussion or clarification of this matter.

Sincerely,

A handwritten signature in dark ink, appearing to read "Steven A. Varga", is written over the typed name.

Steven A. Varga, Chief  
Light Water Reactors Branch No. 4  
Division of Project Management

cc: See next page

Washington Public Power Supply System

ccs:

Joseph B. Knotts, Jr., Esq.  
Debevoise & Liberman  
700 Shoreham Building  
806 Fifteenth Street, N. W.  
Washington, D. C. 20005

Richard Q. Quigley, Esq.  
Washington Public Power Supply System  
3000 George Washington Way  
P. O. Box 968  
Richland, Washington 99352

Nepom & Rose  
Suite 101 Kellogg Building  
1935 S. E. Washington  
Milwaukie, Oregon 97222

Ms. Helen Vozenilek  
7214 S. E. 28th Street  
Portland, Oregon 97202

Ms. Susan M. Garrett  
7325 S. E. Steele Street  
Portland, Oregon 94206

Nicholas Lewis, Chairman  
Energy Facility Site Evaluation Council  
820 East Fifth Avenue  
Olympia, Washington 98504

ATTACHMENT 1

NOV 06 1978

REVIEW GUIDELINES  
TABLE OF CONTENTS

No.	Date	Subject	Rev. No:	Date
1	11/26/77	Screening of Individuals Granted Unescorted Access to the Protected Area		
2	12/20/77	Escorting of Unattended Visiting Vehicles		
3	XX	Performance of Metal Detection Devices	1	2/16/78
4	12/20/77	Performance of X-Ray Devices		
5	XX	Licensee Designated Vehicles	3	11/01/78
6	12/20/77	Need for Access to Vital Areas		
7	2/21/78	Changing of Hard Key/Locks Upon Employee Termination		
8	12/20/77	Criteria for Granting Fewer than 10 Armed Responders		
9	1/2/78	Acceptable Compensatory Measures for Intrusion Detection Hardware Outage (e.g., Zone, System) Protected Area Vital Areas		
10	1/10/78	Compensatory Measures for the Loss of Normal Power Supply to Security Lighting		
11	1/10/78	Vital Area Positive Access Control Definition		
12	1/10/78	Sabotage Incident Management		
13	1/10/78	Compensatory Measures for Vital Areas Lacking the "Two Barrier Protection"		
14	1/17/78	Locking Systems-Assurance of Safety and Safeguards During an Emergency		
15	2/6/78	Package Search		
16	2/2/78	Protective Measures for CAS or SAS Using the Equivalent Information Concept		
17	XX	Definition of Vital Areas	1	1/23/78

NOV 06 1978

REVIEW GUIDELINES  
TABLE OF CONTENTS

No.	Date	Subject	Rev..No.	Date
18	1/6/78	Protected Area Control Function in Bullet Resisting Structure		
19	4/26/78	Manpower Sharing for Operating Reactors		
20	XX	Searching for Explosives	1	4/18/78
21	5/26/78	ID Badge - Vital Area Encoding		
22	5/26/78	Unresolved Issues		
23	11/6/78	Protection of Nuclear Power Plants Against Industrial Sabotage by the Insider		





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

NOV 26 1977

MEMORANDUM FOR: Reactor Safeguards Licensing Branch Members  
Division of Operating Reactors

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

SUBJECT: SCREENING OF INDIVIDUALS GRANTED UNESCORTED ACCESS  
TO THE PROTECTED AREA Review Guidelines #1

Screening of individuals granted unescorted access to the protected area helps establish the trustworthiness of employees, prospective employees, and contractors, and reduces the vulnerability of the facility from the threat of an insider. As a minimum, screening programs should meet the guidance in American National Standard, ANSI N18.17, "Industrial Security for Nuclear Power Plants."

In some cases, licensee and contractor employees may not have been subject to the preemployment screening of ANSI N18.17, but the licensee wishes to grant them unescorted access to the protected area. The reason for not using the screening procedures of ANSI N18.17 is that licensee or contractor may have recently implemented a screening program but determined that persons who were employees on the implementation date need not be subject to preemployment screening as a general rule. Also, a licensee or contractor may transfer an employee to a position subject to the screening program but determine the employee need not be subject to the preemployment screening.

Personnel reliability can be adequately established in such cases by a certain minimum length of time of trustworthy employment. This period of trustworthy employment is considered to be equivalent to the reliability established by preemployment screening by ANSI N18.17 and does not decrease the protection of the facility from the threat of the insider.

Based on these considerations, unescorted access to the protected area may be granted to employees of a licensee and its contractors based on the reliability established by three (3) continuous years of trustworthy employment. This method of establishing reliability is considered to be equivalent to the preemployment screening of ANSI N18.17-1973, Sections 4.1 and 4.2. A licensee's program for granting unes-



NOV 2 5 1977

-2-

corted access to the protected area based on trustworthy employment is acceptable if (a) at least three continuous years of employment of the individual with the licensee or his contractor is documented and (b) the trustworthiness of the individual is determined by a review of the individual's employment record.

*Robert A. Clark*

Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller  
J. M. Elliott





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

DEC 1 1977

MEMORANDUM FOR: Reactor Safeguards Licensing Branch Members, DOR  
FROM: R. A. Clark, Chief, Reactor Safeguards Licensing  
Branch, DOR  
SUBJECT: ESCORTING OF UNATTENDED VISITING VEHICLES - REVIEW  
GUIDELINES #2

The requirement to escort visiting vehicles was included in §73.55 to ensure that an adequate prompt response would be undertaken if a vehicle were used as a weapon against a facility. Escorting of an unattended, visiting vehicle is not needed if adequate alternative measures are taken to assure that the unattended vehicle cannot become such a weapon.

Locking the unattended visiting vehicle and placing the keys in the possession of the security force is adequate to provide assurance that the unattended vehicle cannot become a weapon.

A handwritten signature, likely of R. A. Clark, is written in ink above the typed name.

R. A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller  
J. M. Elliott



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

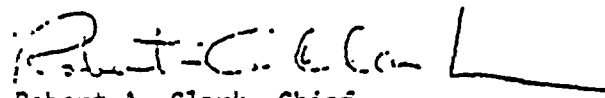
FEB 16 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch, DOR

SUBJECT: PERFORMANCE OF METAL DETECTION DEVICES - REVIEW  
GUIDELINES #3, REVISION 1

All licensees are required to search individuals entering the protected area for firearms. This search is normally conducted by electronic metal detection devices. Enclosed is an acceptable standardized procedure utilizing four specified test weapons. However, this is not to imply that this is the only acceptable test method that can be used to assure proper operation of the devices and that the licensee must purchase four weapons of the type listed. This procedure is designed to detect those weapons most commonly found and covers the spectrum of metal, weight, density, plating, size and shape found in those types of handguns. Other test procedures using test samples other than the type of handgun listed that can demonstrate they can detect the minimum standard of 8 oz., 1/2 lb., or 227 grams of nonferrous metal at the same detection rate for walk-through and hand-held devices as with test weapons will be acceptable.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

Enclosure:  
As stated

cc: J. R. Miller



## Performance of Metal Detection Devices

Purpose To assure that the electronic detection devices (metal detectors) are operating properly through appropriate standardized procedures.

General One method to obtain a decrease in the number of false alarms, is to have all personnel remove all metal before going through the device; that is, place all metallic items in a container and pass this container around the detector.

Responsibility The responsibility for assuring and certifying that the detection device meets the minimum detection standard rests with the using facility. The using facility should maintain a record of the calibrations required to maintain the devices in proper working order.

WALK-THROUGH DETECTION DEVICES The objective of a walk-through detection device is the automatic and reliable detection of any hand guns carried by personnel entering protected area. The subject of the search is only the person, not his hand luggage or other hand-carried items. The detection is to be done automatically at walking speed.

### Performance (Calibration) Test

- a. Walk-through detection devices should be set up at a screening station and the sensitivity set to the level or setting that the manufacturer of the device certifies will cause his type of detector to pass the performance test as specified below. It will be necessary to perform the performance test on initial set up of every device. The test should be performed any time a device fails the operational test described below, each time the device is moved, adjusted, and at least quarterly.
- b. The performance test shall consist of passing the following four weapons at the center line of the detection device passageway four times for each of seven orientations and positions specified for a total of 112 tests. A full performance test should take 15 minutes or less to complete. The tester should be devoid of all practical metal including rings, wrist watches, coins, keys, belt buckles, or other metallic objects. The tester should carry each of the specified test weapons at a normal walking speed through the detection device with the gun barrel oriented in the forward, horizontal and vertical positions at the shoulder, waist, and ankle position except in the latter only the vertical orientation should be used, as shown in Figure 1. The overall detection should be at least 95 detections out of the 112 tests. Sensitivity should



be set to achieve 95 out of 112 successive as a minimum.

- c. The test weapons used for calibration are as follows: Colt .25 Automatic, Titan .25 Automatic, General Precision Model 20 .22 LR, and CDM .22 Short.

Operational Test The objective of the operational test is to ensure that the detecting device is maintained in an operable condition.

- a. Each time the device is turned off or maintained it must be tested prior to being used. If the unit is never turned off, it must be tested at least once every seven days.
- b. The operational test should consist of passing the CDM 22 short weapon held horizontal at the waist three times through the device in the direction of traffic flow through the detector. The detector should signal the presence of the weapon on at least two of the three passes.

HAND-HELD DETECTION DEVICES Detection is indicated by a squealing sound from a loud speaker within the unit when the unit is brought into the vicinity of metal. A squeal will be heard when the unit passes over metal. A high squeal indicates a greater mass of metal is presented.

CALIBRATION PROCEDURES FOR HAND-HELD DEVICES Devices in present use should be calibrated in accordance with manufacturer's instructions.

SUGGESTED SEARCH PROCEDURES FOR THE USE OF ALL HAND-HELD DEVICES

The following procedures should be used in conducting a search using hand-held detection devices.

- a. Assure that the detection device is in proper working order.
- b. With the device approximately two to four inches from the subject, slowly pass the device over the entire body with the detection loop parallel with the body, front and back. Then pass the device slowly over the arms and legs, front, back and sides. Particular attention should be paid to waist, groin, armpit, and ankle area. With practice, a thorough search can be made in one minute. Hand-carried outer garments will be searched by hand. Bags and parcels of any size will not be searched using a hand-held weapon detection device.
- c. If unit alarms, it indicates that metal is present in a given area. Ask subject to remove any metal and search again.

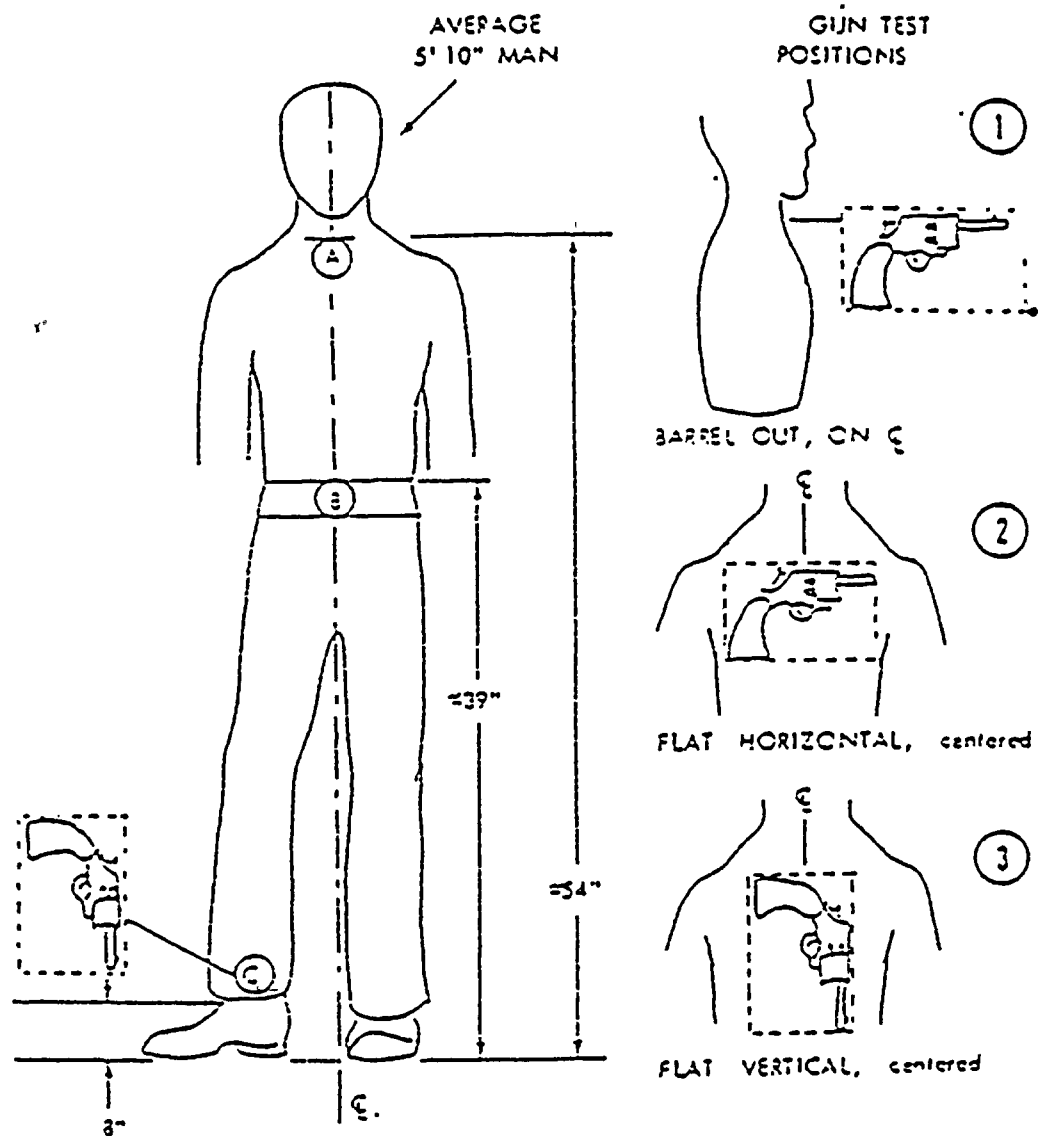
Performance Test The performance test for hand-held detectors should be conducted at the beginning of each shift: The CDM .22 short will be placed in positions 1 through 3 as shown in Figure 1. The detection



should be at least 3 detections out of 3 tests for each position tested.

Operational Test The operational test for hand-held metal detectors is the same as the performance test.





PLANT GUNS IN LOCATION A, B, C, AS FOLLOWS:

- Loc A: Position 1, 2, and 3 with top edge of box as shown by locating dimension.
- Loc B: Position 1, 2, and 3 with top edge of box as shown by locating dimension.
- Loc C: Position 3 with bottom edge of box as shown by locating dimension.

Figure 1





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

DEC 11 1977

MEMORANDUM FOR: Reactor Safeguards Licensing Branch, DOR

FROM: Robert A. Clark, Chief, Reactor Safeguards  
Licensing Branch, DOR

SUBJECT: PERFORMANCE OF X-RAY DEVICES - REVIEW GUIDELINES #4

All licensees are required to search packages entering the protected area. This search may be conducted by X-ray devices. Enclosed is a standardized procedure that is acceptable to assure the X-ray devices are operating properly.

*Robert A. Clark*  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller  
J. M. Elliott





## Performance of X-Ray Devices

### Equipment Performance Standard:

- (1) An X-ray monitor must be able to image and an operator must be able to see an insulated 24 gauge solid copper wire.

### Operator Performance Standard:

- (1) Operators of an X-ray monitor must be trained to recognize unauthorized articles, including weapons, explosives and incendiary devices in X-ray images.

### X-ray Imaging Testing:

- (1) At least quarterly, each X-ray system shall be tested to assure that the monitor will image and an operator can see insulated 24 gauge solid copper wire.
- (2) A wire test kit is used consisting of samples of 20, 22, 24 and 26 gauge solid copper wire.
- (3) The wire test samples are placed in X-ray systems in the same way packages are introduced. If the 26 gauge wire can be seen, the X-ray exceeds performance standards. If the 24 gauge wire can be seen clearly, the X-ray is acceptable. If 22 gauge wire can be seen clearly but not 24 gauge, the X-ray monitor must be repaired or replaced within 48 hours. If 20 gauge wire can be seen but not 22 or 24 gauge, the X-ray monitor must be repaired



or replaced within 24 hours. If 20 gauge wire cannot be seen, the X-ray cannot be used for the screening of packages. Items must be physically inspected.

X-ray Operator Testing:

- (1) An evaluation of operator performance is conducted at least quarterly at each X-ray system. The procedures set forth below are followed using as the test object guns designed for calibration of detector testing. (COLT .25 automatic, Titan .25 automatic, General Precision Model 20.22LR, CPW.22 cal.)
- (2) The test object is positioned in a package so that a clear undisguised lateral (profile) image would logically be projected on the monitor during X-ray inspection of the package.
- (3) The person conducting the test presents the package for inspection just as any person would - without prior notification or identification.
- (4) If the operator detects the object, he or she is appropriately credited.
- (5) If the test object is visible on the monitor and is not detected by the operator, arrangements are made for corrective action such as training, supervision, disciplinary action, etc.
- (6) If a clear image of the test object is not visible on the X-ray monitor, the wire test is conducted to make certain the X-ray is operating satisfactorily. If it is, the operator test is repeated. If not, appropriate corrective action is taken.





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

NOV 01 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch  
Division of Operating Reactors, NRR

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors, NRR

SUBJECT: LICENSEE DESIGNATED VEHICLES - REVIEW GUIDELINE #5  
REVISION THREE

Licensee Designated Vehicles (LDVS) are defined as those vehicles owned by the licensee or owned by a contractor of the licensee. All LDVS are limited in their use to onsite plant functions and remain in the protected area except for operational, maintenance, repair, security, and emergency purposes. All LDVS shall be used only by authorized persons. When unattended, all LDVS shall have the ignition locked and the ignition key controlled by an authorized person.

LDVS shall only be allowed to leave the protected area for the purpose of servicing, repairs, emergencies or other directly related activities. Under these circumstances, a search of the vehicle will be conducted prior to re-entry. However, LDVS may be allowed to leave the protected area and return without being searched providing:

1. The vehicle did not leave the owner-controlled area, and
2. Two individuals having unescorted access to the protected area have been with the vehicle continuously to ensure the vehicle is not being used to transport weapons, explosives or incendiary devices into the protected area.

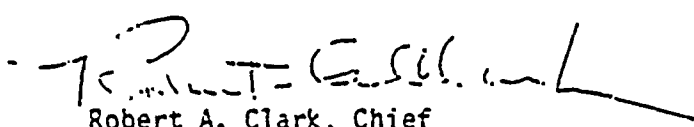
OR

1. The vehicle does not leave the owner-controlled area, and
2. The vehicle and driver are under the surveillance of a member of the security organization to ensure that no contraband is placed in or on the vehicle while outside the protected area.



NOV 01 1978

Licensee or contractor owned vehicles (particularly special purpose vehicles) that are not normally assigned to onsite plant functions may be so designated as LDVS temporarily for short periods (but not less than 24 hours) provided they are searched prior to entry and are subjected to the same controls as permanent LDVS.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors, NRR

cc: J. R. Miller



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

DEC 20 1977

MEMORANDUM FOR: Reactor Safeguards Licensing Branch, DOR

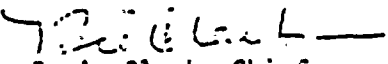
FROM: R. A. Clark, Chief, Reactor Safeguards  
Licensing Branch, DOR

SUBJECT: NEED FOR ACCESS TO VITAL AREAS - REVIEW GUIDELINE #6

Positive access control is required for the physical protection of nuclear power plants. Positive access control provides assurance that only authorized individuals enter a vital area for authorized reasons. One element of positive access control is the establishment of the need for access. A system for establishing the need for access should be based on an individual's assigned duties and normal working hours. During normal working hours an individual should be granted access based upon his position. It is not necessary to determine his exact reason to enter a vital area that is associated with his assigned tasks. During times other than normal working hours an individual should confirm a need to enter a vital area. The following describes an acceptable method of establishing a need for access to vital areas.

Need for Access

- (1) The need for access is established when an individual is authorized access to vital areas. This need for access is revalidated at least once every 31 days. During normal working hours, an individual is granted access to those vital areas identified in his authorization.
- (2) The shift supervisor is notified of all individuals on site more than one hour after the end of the individual's normal working hours. No further action is required unless directed by the shift supervisor.
- (3) The shift supervisor is notified prior to granting an individual access to the protected area at times other than the individual's normal reporting time. When granting access to the protected area, the shift supervisor may also grant access to those vital areas identified in the individual's authorization.

  
R. A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller  
J. M. Elliott





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

FEB 21 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors, NRR

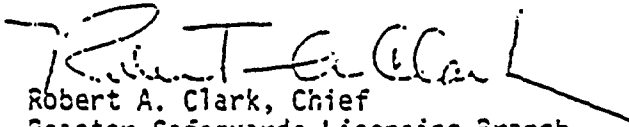
SUBJECT: CHANGING OF HARD KEY/LOCKS UPON EMPLOYEE  
TERMINATION - REVIEW GUIDELINE NUMBER 7

10 CFR 73.55 requires that all keys, locks, combinations and related equipment used to control access to protected and vital areas be controlled to reduce the probability of compromise. The rule also requires that whenever there is evidence that any key, lock, combination may have been compromised, it shall be changed. The rule proceeds to require that upon termination of employment of any employee, the keys, locks, combinations and related equipment to which the employee had access shall be changed.

The objective of changing keys, locks, combinations and related equipment upon termination of an employee is to reduce the probability of compromise. For a hard (metal) key and lock system, the objective of reducing the probability of compromise of the keys and locks can be met by a program that changes hard keys and locks on a periodic basis and upon termination of an employee for other than favorable reasons.

The following describes an acceptable method of changing hard keys, locks and related equipment to which a terminated employee had access:

- (1) If an employee is terminated under other than favorable conditions, all keys, locks and related equipment to which he had access shall be changed.
- (2) The keys, locks and related equipment to which a terminated employee had access need not be changed if:
  - (a) The termination was under favorable conditions and the licensee documents this fact, and
  - (b) The licensee periodically (at least once each 12 months) changes or rotates all hard keys and locks for the protected area barrier and all access doors to vital areas.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch



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

DEC 29 1977

MEMORANDUM FOR: Reactor Safeguards Licensing Branch, DOR

FROM: R. A. Clark, Chief, Reactor Safeguards  
Licensing Branch, DOR

SUBJECT: CRITERIA FOR GRANTING FEWER THAN 10 ARMED  
RESPONDERS - REVIEW GUIDELINE #8

The regulations provide for a nominal number of armed response personnel as ten (10) and that this number may not be reduced to less than five (5) guards. The statement of consideration states that the number of such personnel may be more or less than the nominal number depending on factors such as the following, to be considered during evaluation of a licensee's physical security plan, not necessarily in order of importance:

- (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 LLEA response.
- (g) Vital area hardening, including plant design, location of and access control to vital areas.
- (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.

In addition to these criteria, the following factors may be considered to evaluate the case by case justification for response personnel numbers:

- (a) The LLEA response time and their numbers.
- (b) The quality of the screening program.
- (c) The complexity of the layout of the plant within the protected area.
- (d) The analysis of the integrated security system as described in NUREG 0220, Chapter 11.



Reactor Safeguards Licensing  
Branch

-2-

- (e) Factors outside the owner controlled area that may increase or decrease the vulnerability of the protected area and are beyond the licensee's control.
- (f) The availability of guards or response personnel from other guard forces in the vicinity.

*R. A. Clark*

R. A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller  
J. M. Elliott





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

JAN 1378

MEMORANDUM FOR: Reactor Safeguards Licensing Branch Members, DOR

FROM: Robert A. Clark, Chief, Reactor Safeguards  
Licensing Branch, DOR

SUBJECT: ACCEPTABLE COMPENSATORY MEASURES FOR INTRUSION DETECTION  
HARDWARE OUTAGE (E.G., ZONE, SYSTEM) PROTECTED AREA  
VITAL AREAS - REVIEW GUIDELINE NUMBER 9

The objective of perimeter intrusion detection hardware is to detect the unauthorized entry or attempted entry of individuals or vehicles into the protected area and to provide an "alert" to the security organization so that response by a response force will be initiated at the time of penetration into the protected area.

In the event of a hardware outage the compensatory measures must satisfy this objective by providing a means for detecting unauthorized entry and for alerting the security organization or by providing a response force to control all paths from the area of outage to all vital areas. Acceptable measures compensatory to perimeter intrusion detection outage are:

- a) Back-up intrusion detection system of equal capability.
- b) Dedicated CCTV with continuous monitoring of the perimeter zone(s) affected by the outage.
- c) On-the-spot guards visually monitoring the perimeter zone(s) affected by the outage.
- d) Response force deployed to control all paths from the perimeter zone(s) affected by the outage to all vital areas.

The objective of the vital area intrusion detection hardware is to detect the unauthorized entry of individuals (and at some facilities - vehicles) into vital areas and to provide to the security organization an "alert" so that response by a response force will be initiated at the time of penetration into the vital area.

In the event of a hardware outage the compensatory measures must satisfy this objective by either providing a means for detecting unauthorized

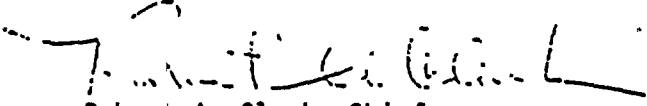


Reactor Safeguards Licensing  
Branch Members

-2-

entry and alerting the security organization or providing the response force to control the paths to the affected vital areas. Acceptable measures compensatory to a vital area intrusion detection outage are:

- a) A back-up intrusion detection system of equal capability.
- b) Dedicated CCTV with continuous monitoring of the portals affected by the outage.
- c) On-the-spot guards visually monitoring the portals affected by the outage.
- d) Response force deployment to control all approaches to the affected vital areas.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors



*[Faint handwritten notes]*



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

JAN 10 1972

MEMORANDUM FOR: Reactor Safeguards Licensing Branch


FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

SUBJECT: COMPENSATORY MEASURES FOR THE LOSS OF NORMAL  
POWER SUPPLY TO SECURITY LIGHTING - REVIEW  
GUIDELINE NUMBER 10

Illumination, as an element of a security sys-  
tem, is a security organization with the capability to  
protect a protected area to permit early detection and  
to a limited extent acts as a deterrent to potential  
the loss of this element, certain compensatory measures  
implemented to counteract the deficiency.

The following represent some of the acceptable compensatory measures  
which when utilized separately or in combination, would be found  
appropriate:

- 1) Switch to stand-by power.
- 2) Low light level surveillance devices.
- 3) Portable lighting devices.
- 4) Positioning of security personnel at strategic locations  
for adversary interception.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch



F-12



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

JAN 11 1978

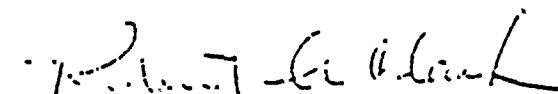
MEMORANDUM FOR: Reactor Safeguards Licensing Branch

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

SUBJECT: VITAL AREA POSITIVE ACCESS CONTROL DEFINITION -  
REVIEW GUIDELINE NUMBER 11

Positive Access Control is defined as those measures necessary to assure that individuals who request entry into vital areas have been determined to have a need for such access and that these individuals have been positively identified before entry is granted into those areas.

For vital areas, positive access control is accomplished upon entry into the Protected Area where personnel are positively identified as having a need for access and "keys" are issued for vital areas according to the assessed need.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing  
Branch





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

F.12

JAN 11 1975

MEMORANDUM FOR: Reactor Safeguards Licensing Branch

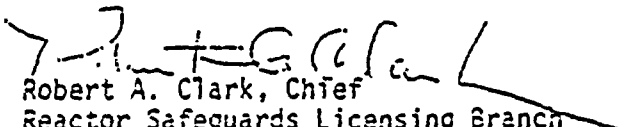
FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

SUBJECT: SABOTAGE INCIDENT MANAGEMENT - REVIEW GUIDELINE  
NUMBER 12

The licensee is responsible for the safe operation of his nuclear power plant and therefore is obligated to employ effectively all resources within his control to protect the public health and safety under all circumstances, including a sabotage incident.

The security plans and procedures implementing the security plans prescribe the means to provide protection with high assurance against successful industrial sabotage by two design level threats (§73.55 (a)(1)(2)). The protection thus afforded is not limited to the design level threats, but will also provide a lesser or greater degree of protection for threats that are larger or smaller, simpler or more sophisticated.

In the event of a sabotage attempt, the available licensee and LLEA resources and forces must be used in the most effective manner to counter the actual threat based on the circumstances of the situation. It is recognized that the Security Plan and the implementing security procedures may not equally or adequately address the complete range of possible threats. Therefore, it is necessary that the security plan and procedures accommodate the necessary freedom of action needed by the individual in charge at the site at time of an actual threat to employ the available resources (e.g. physical protection systems, security organization, response forces, LLEA, etc) in a manner that he considers most effective to counter that threat.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch





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

F-12

JAN 17 1979

MEMORANDUM FOR: Reactor Safeguards Licensing Branch

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

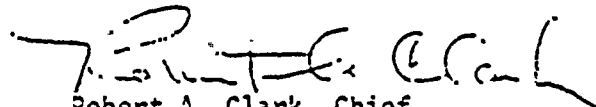
SUBJECT: COMPENSATORY MEASURES FOR VITAL AREAS LACKING  
THE "TWO BARRIER PROTECTION" - REVIEW GUIDELINE  
NUMBER 13

10 CFR 73.55 requires that vital equipment be protected by a minimum of two barriers i.e., Protected and Vital, which are defined in 10 CFR 73.2. The barriers coupled with the defense in depth concept, isolation zones, continuous monitoring and periodic surveillance result in high assurance detection and resistance to penetration.

In some cases barrier separation is impossible to achieve due to operational design needs, as exemplified most often by the positioning of the service water intake structures on borders of bodies of water. In other cases location of vital equipment was instituted prior to the issuance of 73.55, making it impractical to require relocation. In both cases other measures must be implemented to compensate for the loss of the basic criteria.

The following represent some acceptable compensatory (or equivalent) measures that may be used together or separately (depending upon site specifics) in achieving the objective:

1. Hardening of common barriers.
2. Additional "early warning" monitoring devices.
3. More frequent surveillance.
4. Positive response posture to common barrier locations.
5. Positioning of security post in close proximity of common barriers.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch







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

MEMORANDUM FOR: Reactor Safeguards Licensing Branch

FROM: R. A. Clark, Chief  
Reactor Safeguards Licensing Branch

SUBJECT: LOCKING SYSTEMS-ASSURANCE OF SAFETY AND SAFEGUARDS  
DURING AN EMERGENCY-REVIEW GUIDELINE NUMBER 14

Under emergency conditions, prompt ingress into certain safety-related areas must be assured to enable safe shutdown of a nuclear power plant, and unimpeded egress from all parts of the facility must be assured in the interest of personnel safety.

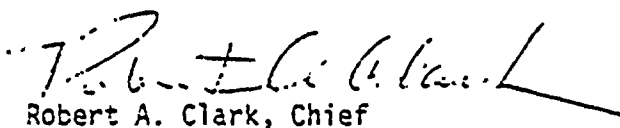
The design and operation of security devices for doors to vital areas should be based on both safety and security. The following provides guidance on the design and use of security devices on vital area doors:

- a) Prompt emergency ingress into electrically and mechanically locked-safety-related areas by essential personnel must be assured in any postulated occurrence through the combined use of the features below or, the equivalent.
  - 1) Provide reliable and uninterruptable auxiliary power to the entire electrical locking system, including its controls (sufficient physical separation, electrical isolation, and redundancy must be provided to prevent the occurrence of a common mode failure in the uninterruptable auxiliary power supply for the lock system in any design basis event); and
  - 2) Provide electrical locking devices which fail in the secure mode upon loss of both primary and auxiliary power and are equipped with secure mechanical means and associated procedures to override the failed electrical locking devices (e.g., key locks with keys held by appropriate personnel who know when and how to use them); or
  - 3) Provide electrical locking devices which fail in the open mode upon loss of both primary and auxiliary power and associated procedures which provide compensatory measures for the open doors (e.g., deploying guards to strategic points)



(The fail open feature should be used only on selected interior doors.); or

- 4) Provide key locks with keys held by appropriate personnel who know when and how to use them; and
  - 5) Provide periodic testing of all locking systems and mechanical overrides to confirm their operability under auxiliary power as well as failed conditions.
- b) Unimpeded emergency egress must be assured from all parts of facilities, the security hardware and systems must be designed and installed so as to not degrade personnel safety, and such hardware and systems should be in conformance with applicable (State/Local) fire regulations and life safety codes.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch





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

FEB 6 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch; DOR

FROM: R. A. Clark, Chief  
Reactor Safeguards Licensing Branch, DOR

SUBJECT: PACKAGE SEARCH - REVIEW GUIDELINE NUMBER 15

Paragraph 73.55 (d)(3) requires that all packages and material for delivery into the protected area shall be checked for proper identification and authorization and searched for devices such as firearms, explosives and incendiary devices or other items which could be used for industrial sabotage prior to admittance into the protected area, except those Commission approved delivery and inspection activities specifically designated by the licensee to be carried out within vital or protected areas for reasons of safety, security or operational necessity.

This requirement ensures detection of unauthorized materials before protected area entry or before they could be effectively employed in industrial sabotage of vital equipment. The following provides guidance for meeting the requirements of § 73.55 (d)(3) and for Commission approval of delivery and inspection activities inside the protected area:

- (1) All packages and material for delivery into the protected area shall be checked for proper identification and authorization.
- (2) Prior to entering the protected area all packages and material shall be physically searched, machine searched or handled as one of the categories listed below.

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

- (1) the vehicle is escorted by a guard, and
- (2) the packages and material is under the observation of a guard, and
- (3) the packages and materials are not unloaded in the protected area.

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




FEB 06 1978

RSLB

- 2 -

Category III - Packages and materials excluded from search because search constitutes a danger to the individual or would render the object being searched unusable or contaminated. These packages and materials shall be positively controlled. (For example, stored in a locked area controlled by persons familiar with the material). Products for human consumption shall be positively controlled only to the extent practical. (For example, limiting most items to the lunch room)

Category IV - Packages and materials 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 contents.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

Enclosure:  
List of Examples of Each Category

cc: J. R. Miller





## Examples of Each Category

### Category I

Packages on common carrier vehicles, such as UPS  
Packages on vendor vehicles, such as drinks and food consigned to other locations  
Garbage pickup trucks  
Waste oil removal trucks  
Sewage pumping vehicles

### Category II

Gravel  
Lumber, Paving material  
Fill dirt  
Iron & steel pipe, angles, sheet  
Gasoline  
Carbon dioxide  
Diesel fuel  
Hydrogen  
Nitrogen (liquid)  
Power transformer oil  
Turbine oil  
Propane gas  
Sodium hydroxide  
Sulfuric acid  
Pressurized gas cylinders  
Resins

### Category III

Small individually packaged food container  
Canned drinks for human consumption  
Cigarettes  
Fuel assemblies

### Category IV

Office supplies  
Machine sealed or factory assembled materials and equipment  
Hermetically sealed products



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

FEB 02 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

SUBJECT: PROTECTIVE MEASURES FOR CAS OR SAS USING THE EQUI-  
VALENT INFORMATION CONCEPT-REVIEW GUIDELINE NUMBER 16

§73.55 requires, in part, the assessment of a threat; response to detection of a penetration or an intrusion; and a capability of observing isolation zones and the physical barrier at the perimeter of the protected area. The detection aids, communications and response requirements in §73.55 (e), (f) and (h) were intended to assist the licensee by providing him with an acceptable means of meeting these responsibilities. Paragraph (e) requires two continuously manned alarm stations so that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm; that all alarms shall annunciate in both stations; and shall indicate the type and location of each alarm. Paragraph (f) requires that both alarm stations shall have two-way voice communications as well as conventional telephone communication. Paragraph (h) requires a surveillance capability. These requirements have been interpreted to mean that the licensee must provide for the receipt and display of equivalent alarm and surveillance data plus communications capability in both alarm stations but not necessarily the same level of surveillance monitoring display.

The following are the regulatory requirements for the CAS & SAS:

- (1) Both stations shall be continuously manned.
- (2) All alarms must annunciate in both stations.
- (3) Annunciation shall indicate type and location of alarm.
- (4) Both stations must have two-way voice (wireless) as well as conventional telephone capability.
- (5) Both stations must have equivalent alarm and surveillance data.
- (6) All alarm devices and alarm transmission lines for both stations must be self-checking and tamper-indicating.



FEB 02 1978

Since §73.55 does not provide guidance on how these stations are to interact, protecting against the threat of an insider operating from either station will have to be dealt with through licensee developed procedural checks designed to insure against successful malevolent actions by either alarm station operator. However, criteria have evolved that appear essential in establishing a defensive frame work against this threat. Consequently the following additional licensee implemented measures, used individually or in combination, when coupled with the regulatory requirements set forth above, are acceptable in satisfying the high assurance provisions of §73.55 (a)(2).

- (1) Random selection of CAS/SAS operators at the beginning of each shift.
- (2) Use of the two-man rule in CAS.
- (3) Each station to have independence of action to call for assistance when suspicious of the action(s) of the other station.
- (4) The secondary station must have the capability of confirming the appropriateness of the CAS operators actions in response to alarms (e.g., radio contact with responders, surveillance monitoring, etc.).
- (5) Strict control of access to the security computer software programs.
- (6) Strict control of access to either station.
- (7) Insuring that one station cannot inhibit the flow of information to the other.

The foregoing are not meant to be all inclusive. They are listed as the most desired licensee actions that when coupled with the regulatory requirements set forth above will provide the high assurance protection that is being sought.



Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch



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

JAN 23 1975

MEMORANDUM FOR: Reactor Safeguards Licensing Branch  
Members, DOR

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch, DOR

SUBJECT: DEFINITION OF VITAL AREAS, REVISION 1 -  
REVIEW GUIDELINE NO. 17

Enclosed is Review Guideline Number 17, i.e., the  
revised definition of vital areas.

*Robert A. Clark*  
Robert A. Clark, Chief  
Reactor Safeguards Licensing  
Branch, DOR

Enclosure:  
As stated



DEFINITION OF  
VITAL AREAS AND EQUIPMENT  
Revision 1

A. Applicable Sections of 10 CFR 73

73.55 (c)(1):

"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 of sufficient strength to meet the performance requirements of paragraph (a) of this section. More than one vital area may be located within a single protected area."

73.2 (h):

"Vital area means any area which contains vital equipment within a structure, the walls, roof, and floor of which constitute physical barriers of construction at least as substantial as walls as described in paragraph (f)(2)."

73.2 (i):

"Vital equipment means any equipment, system, device, or material failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to function to protect public health and safety following such failure, destruction or release are also considered to be vital."



B. Assumptions and Definitions

In the application of these regulations to a typical LWR plant, the following considerations and assumptions are made:

1. Paragraph 73.55 (c) requires vital equipment to be enclosed by two barriers. The combination of barriers, in conjunction with other components of the security system, must provide a sufficient delay to an intrusion to meet the performance requirements of 73.55 (a).
2. To "endanger the public health and safety by exposure to radiation" requires a significant off-site release of radioactivity. For LWR's the following sources of significant quantities of radioactivity should be considered:
  - a. The reactor core,
  - b. Spent fuel,
  - c. Radwaste systems, if the total radwaste inventory is greater than  $nxC$ , where:
    - n is the ratio of the applicable dose guideline of 10 CFR 100 to the dose computed for accidental releases in Chapter 15 of the FSAR, and
    - c is the release (curies) assumed in the accidental release calculation of the FSAR.
3. Vital Areas fall into two general categories:
  - a. Type I vital areas, i.e., those areas wherein successful sabotage can be accomplished by compromising or destroying

the vital systems<sup>1/</sup> or components located within this area. (By definition, an area containing systems or components whose failure or destruction results in a direct release is a Type I vital area.)

- b. Type II vital areas, ie., those areas which contain systems or components whose failure or destruction would lead to successful sabotage only in conjunction with additional sabotage activity in at least one other, separate<sup>2/</sup> vital area. (Safety related equipment designed to mitigate the consequences of failures of other systems usually falls into this category.)

4. When classifying vital equipment as Type I or II, the following assumptions apply:

- a) The concurrence of violent natural phenomena with a security contingency need not be considered.
- b) Random (accidental) failure of equipment concurrent with a security contingency need not be considered. However, a security contingency during routine or planned outages of equipment, as permitted by the technical specifications, must be considered.

1/ "System" refers to all components, mechanical and electrical, including piping, cabling, power supply, and other support systems to carry out the design function provided by the system.

2/ For the purpose of this discussion, a vital area may be considered "separate" if it is separated from the area under consideration by a barrier or distance sufficient to delay the saboteur's access long enough to demonstrate interception and engagement by the security response force.

- c) Loss of off-site power must be assumed since it is impractical to protect transmission lines against sabotage.

C. Discussion

The definition of vital equipment, 73.2 (i), includes equipment whose failure would lead to a direct release, as well as equipment required to function for the protection of public health and safety following a postulated sabotage attack. This is analagous to the definition of safety-related equipment, which includes primary fission product barriers, as well as the systems required to mitigate the consequences of a breach of the barrier. Therefore, essentially all safety related equipment must be considered vital. In order to avoid duplication of safety analyses, the systems listed in Reg. Guide 1.29 should be considered vital.

It should be noted that a facility which provides sufficient delay time to permit interruption of the external threat of s(a)(1) at all vital area barriers, and for which adequate protection against the insider threat of s(a)(2) is provided for all vital areas would meet the requirements of 73.55 without the designation of any Type I Vital Areas. In practice, however, it is to the licensee's advantage to segregate vital areas into Type I and II, in order to take credit for the fact that a saboteur could not achieve successful sabotage in Type II vital areas without penetrating additional barriers.



D. Review Guidelines

1. All systems listed in Reg. Guide 1.29 as "Seismic Category I" are considered vital. (A sound technical basis must be provided by the licensee for any deviation from this list.)
2. Type I Vital Areas should be identified by the licensee, using the definitions and assumptions listed in B. If Type I Vital Areas are not identified by the licensee, the list provided in the Appendix may be used as guidance.
3. High assurance protection against the external and internal threat must be provided for all Type I Vital Areas. This requires a demonstration that any external Type I vital barriers provide sufficient delay to the external threat (§(a)(1)) to permit a timely engagement by the armed response force, and appropriately restricted access controls, controls of activity, or other methods of protection against the insider, to meet the internal threat (§(a)(2)). For Type II Vital Areas, a combination of multiple barriers, each of which meets the requirements of 73.2(f)(2) or its equivalent, and the associated individual access controls, provides high assurance protection against the external and internal threat.

Appendix

SAMPLE LIST OF TYPE I VITAL AREAS

1. Primary containment
2. Containment electrical and piping penetration areas
3. Control room
4. Cable spreading room
5. Primary shutdown system (if outside containment)
6. All areas associated with one complete decay heat removal system (including all necessary support systems, e.g., power supply, cooling, and lubricating systems.)
7. Battery rooms (including battery charger areas)

**REGULATORY GUIDE**

OFFICE OF STANDARDS DEVELOPMENT

## REGULATORY GUIDE 1.29

**SEISMIC DESIGN CLASSIFICATION****A. INTRODUCTION**

General Design Criterion 2, "Design Bases for Protection Against Natural Phenomena," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50, "Licensing of Production and Utilization Facilities," requires that nuclear power plant structures, systems, and components important to safety be designed to withstand the effects of earthquakes without loss of capability to perform their safety functions.

Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 establishes quality assurance requirements for the design, construction, and operation of nuclear power plant structures, systems, and components that prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. The pertinent requirements of Appendix B apply to all activities affecting the safety-related functions of those structures, systems, and components.

Appendix A, "Seismic and Geologic Site Criteria for Nuclear Power Plants," to 10 CFR Part 100, "Reactor Site Criteria," requires that all nuclear power plants be designed so that, if the Safe Shutdown Earthquake (SSE) occurs, all structures, systems, and components important to safety remain functional. These plant features are those necessary to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the guideline exposures of 10 CFR Part 100.

This guide describes an acceptable method of identifying and classifying those features of light-water-cooled

nuclear power plants that should be designed to withstand the effects of the SSE.

**B. DISCUSSION**

After reviewing a number of applications for construction permits and operating licenses for boiling and pressurized water nuclear power plants, the NRC staff has developed a seismic design classification system for identifying those plant features that should be designed to withstand the effects of the SSE. Those structures, systems, and components that should be designed to remain functional if the SSE occurs have been designated as Seismic Category I.

**C. REGULATORY POSITION**

1. The following structures, systems, and components of a nuclear power plant, including their foundations and supports, are designated as Seismic Category I and should be designed to withstand the effects of the SSE and remain functional. The pertinent quality assurance requirements of Appendix B to 10 CFR Part 50 should be applied to all activities affecting the safety-related functions of these structures, systems, and components.

- a. The reactor coolant pressure boundary.
- b. The reactor core and reactor vessel internals.

c. Systems<sup>1</sup> or portions of systems that are required for (1) emergency core cooling, (2) postaccident containment heat removal, or (3) postaccident

<sup>1</sup>The system boundary includes those portions of the system required to accomplish the specified safety function and connected piping up to and including the first valve (including a safety or relief valve) that is either normally closed or capable of automatic closure when the safety function is required.

**USNRC REGULATORY GUIDES**

Regulatory Guides are issued to describe and make available to the public methods acceptable to the NRC staff of implementing specific parts of the Commission's regulations. To demonstrate techniques used by the staff in evaluating specific problems or postulated accidents, or to provide guidance to applicants. Regulatory Guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings required to the issuance or continuance of a permit or license by the Commission.

Comments and suggestions for improvements in these guides are encouraged at all times, and guides will be revised as appropriate in accordance with comments and to reflect new information or experience. However, comments on this guide, received within about two months after its issuance, will be particularly useful in evaluating the need for an early revision.

Comments should be sent to the Secretary of the Commission, U.S. Nuclear Regulatory Commission, Washington, D.C. 20556, Attention: Secretary and Service Section.

The guides are issued in the following ten broad divisions:

- |                                   |                        |
|-----------------------------------|------------------------|
| 1. Power Reactors                 | 6. Products            |
| 2. Research and Test Reactors     | 7. Transportation      |
| 3. Fuels and Materials Facilities | 8. Occupational Health |
| 4. Environmental and Siteing      | 9. Antitrust Review    |
| 5. Materials and Plant Protection | 10. General            |

Copies of published guides may be obtained by written request indicating the guides desired to the U.S. Nuclear Regulatory Commission, Washington, D.C. 20556, Attention: Director, Office of Standards Development.

containment atmosphere cleanup (e.g., hydrogen removal system).

d. Systems<sup>1</sup> or portions of systems that are required for (1) reactor shutdown, (2) residual heat removal, or (3) cooling the spent fuel storage pool.

e. Those portions of the steam systems of boiling water reactors extending from the outermost containment isolation valve up to but not including the turbine stop valve, and connected piping of 2-1/2 inches or larger nominal pipe size up to and including the first valve that is either normally closed or capable of automatic closure during all modes of normal reactor operation. The turbine stop valve should be designed to withstand the SSE and maintain its integrity.

f. Those portions of the steam and feedwater systems of pressurized water reactors extending from and including the secondary side of steam generators up to and including the outermost containment isolation valves, and connected piping of 2-1/2 inches or larger nominal pipe size up to and including the first valve (including a safety or relief valve) that is either normally closed or capable of automatic closure during all modes of normal reactor operation.

g. Cooling water, component cooling, and auxiliary feedwater systems<sup>1</sup> or portions of these systems, including the intake structures, that are required for (1) emergency core cooling, (2) postaccident containment heat removal, (3) postaccident containment atmosphere cleanup, (4) residual heat removal from the reactor, or (5) cooling the spent fuel storage pool.

h. Cooling water and seal water systems<sup>1</sup> or portions of these systems that are required for functioning of reactor coolant system components important to safety, such as reactor coolant pumps.

i. Systems<sup>1</sup> or portions of systems that are required to supply fuel for emergency equipment.

j. All electric and mechanical devices and circuitry between the process and the input terminals of the actuator systems involved in generating signals that initiate protective action.

k. Systems<sup>1</sup> or portions of systems that are required for (1) monitoring of systems important to safety and (2) actuation of systems important to safety.

l. The spent fuel storage pool structure, including the fuel racks.

m. The reactivity control systems, e.g., control rods, control rod drives, and boron injection system.

n. The control room, including its associated vital equipment, cooling systems for vital equipment, and life support systems, and any structures or equipment inside or outside of the control room whose failure could result in incapacitating injury to the occupants of the control room.<sup>2</sup>

o. Primary and secondary reactor containment.

p. Systems<sup>1</sup> other than radioactive waste management systems,<sup>3</sup> not covered by items 1.a through 1.o above that contain or may contain radioactive material and whose postulated failure would result in conservatively calculated potential offsite doses (using meteorology as prescribed by Regulatory Guide 1.3, "Assumptions Used for Evaluating the Potential Radiological Consequences of a Loss of Coolant Accident for Boiling Water Reactors," and Regulatory Guide 1.4, "Assumptions Used for Evaluating the Potential Radiological Consequences of a Loss of Coolant Accident for Pressurized Water Reactors") that are more than 0.5 rem to the whole body or its equivalent to any part of the body.

q. The Class 1E electric systems, including the auxiliary systems for the onsite electric power supplies, that provide the emergency electric power needed for functioning of plant features included in items 1.a through 1.p above.

2. Those portions of structures, systems, or components whose continued function is not required but whose failure could reduce the functioning of any plant feature included in items 1.a through 1.q above to an unacceptable safety level should be designed and constructed so that the SSE would not cause such failure.

3. Seismic Category I design requirements should extend to the first seismic restraint beyond the defined boundaries. Those portions of structures, systems, or components that form interfaces between Seismic Category I and non-Seismic Category I features should be designed to Seismic Category I requirements.

4. The pertinent quality assurance requirements of Appendix B to 10 CFR Part 50 should be applied to all activities affecting the safety-related functions of those portions of structures, systems, and components covered under Regulatory Positions 2 and 3 above.

<sup>1</sup>Lines indicate substantive changes from previous issue.

<sup>2</sup>Wherever practical, structures and equipment whose failure could possibly cause such injuries should be relocated or separated to the extent required to eliminate this possibility.

<sup>3</sup>Specific guidance on seismic requirements for radioactive waste management systems is under development.

<sup>1</sup> See footnote 1, p. 1.29-1.





#### D. IMPLEMENTATION

The purpose of this section is to provide information to applicants regarding the NRC staff's plans for using this regulatory guide.

This guide reflects current NRC staff practice. Therefore, except in those cases in which the applicant

proposes an acceptable alternative method for complying with specified portions of the Commission's regulations, the method described herein is being and will continue to be used in the evaluation of submittals for operating license or construction permit applications until this guide is revised as a result of suggestions from the public or additional staff review.



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

FEB 06 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch, DOR

FROM: R. A. Clark, Chief  
Reactor Safeguards Licensing Branch, DOR

SUBJECT: PROTECTED AREA CONTROL FUNCTION IN BULLET-  
RESISTING STRUCTURE-REVIEW GUIDELINE #18

Paragraph 73.55 (d)(1) requires in part, that the individual responsible for the last access control function (controlling admission to the protected area) shall be isolated within a bullet-resisting structure to assure their ability to respond or to summon assistance. The isolation of an individual with the last control function is to preclude an opportunity for forceful or threat of forceful coercion to gain unauthorized entry. Generally this individual operates an electrically operated lock on the main access portal.

Vehicle gates and emergency exits, only used occasionally, may have the access controlled by two guards at the gate/exit provided:

- (a) Individuals are processed through the normal personnel access controls.
- (b) The vehicles are subjected to prior processing at the normal vehicle control station.
- (c) The material and packages on the vehicle have been checked for identification and authorization and have been subjected to search requirements.
- (d) Keys used for unlocking the protected area portal are issued to a guard from within a bullet-resisting structure and are always returned to the bullet-resisting structure after locking the portal.

A handwritten signature in dark ink, appearing to read "Robert A. Clark".

Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller





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

APR 26 1973

MEMORANDUM FOR: Reactor Safeguards Licensing Branch

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

SUBJECT: MANPOWER SHARING FOR OPERATING REACTORS -  
REVIEW GUIDELINE NO. 19

The NRC has established requirements for personnel at a single unit operating nuclear power plant for purposes of plant operation, industrial security and fire fighting. The following discussion considers the extent to which security personnel may also be temporarily allowed to man a fire brigade in the event of a fire.

It is reasonable to allow a limited amount of sharing of plant personnel in satisfying the requirements of plant operation, security and fire protection. An acceptable sharing scheme would entail reliance on some members of the security organization to constitute the fire brigade. Since availability of the full fire brigade would only be required for the most serious fires, actual distribution of plant personnel during a plant emergency would be governed by the exigencies of the situation. It should be recognized that the diversion of security personnel to the fire brigade would be of short duration and that substantial additional offsite assistance would be forthcoming in accordance with the emergency and contingency plans developed for each facility.

In the event of a fire, a contingency plan and procedures will be used in deploying the security organization to assure that an appropriate level of physical protection is maintained during the event. The staff has determined that it is possible in the planning for site response to a fire, to assign a maximum of three members of the security organization to serve on the fire brigade and still provide an acceptable level of physical protection. While certain security posts must be manned continuously (e.g. CAS, SAS), the personnel in other assignments, including the response force, could be temporarily (i.e. 30 minutes) assigned to the fire brigade.

For a multi-unit facility, the extent to which security personnel assigned to man a fire brigade in the event of a fire must be



Reactor Safeguards Licensing Branch - 2 -

determined on a case-by-case basis because of the various sharing schemes that can be used by multi-unit sites. The previous discussion should be considered when determining the maximum number of security organization members to serve on the fire brigade and still provide an acceptable level of physical protection for multi-unit sites.

A handwritten signature in dark ink, appearing to read "Robert A. Clark", with a long horizontal flourish extending to the right.

Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors



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

APR 18 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch

FROM: R. A. Clark, Chief  
Reactor Safeguards Licensing Branch

SUBJECT: SEARCHING FOR EXPLOSIVES -  
REVIEW GUIDELINE NUMBER 20,  
REVISION 1

Background

Paragraph (d)(1) of 10 CFR 73.55 states that "the search for detection of firearms, explosives, and incendiary devices shall be conducted either by physical search or by use of equipment capable of detecting such devices."

The amendment to 73.55(d)(1) published in the September 30, 1977 Federal Register provides interim relief from having to pat-down search regular plant employees entering nuclear power plants provided that equipment designed for detection of weapons and explosive material is utilized to perform the search function on regular plant employees. A copy of the September 30, 1977 Federal Register notice was transmitted as an enclosure to a letter from Edson G. Case to all licensees (11/23/77). Also included was an enclosure "NRR Supplemental Staff Position on Personnel Search Requirements", which further clarified the staff position on personnel searches. This position paper recognized that not all licensees possessed the necessary equipment to conduct the searches on regular employees and therefore provided an alternative (random search procedures) to the use of such equipment. It was never intended however, that these random search procedures be substituted indefinitely for the weapons and explosives detecting equipment. In fact, the staff position paper made it explicitly clear that acceptable metal detectors and explosive searching devices of the types currently available are deemed capable of detecting firearms, explosives and incendiary devices for regular employees of the licensee at the site and that such equipment, if not currently in operation, must be purchased and made operational as soon as possible if the licensee is to be in compliance with the performance requirement of 10 CFR 73.55.





Reactor Safeguards Licensing Branch - 2 -

The staff is not presently aware of any additional information or factors that will result in a change to the position that use of explosive and metal detecting equipment will satisfy the search requirement for regular plant employees.

It is recognized that currently available explosive detection devices (1) are not capable of detecting all types of available explosives and (2) generally operate on principles (vapor detection) that allow for straightforward avoidance techniques by knowledgeable individuals.

Performance Requirements

An explosives detector, or system of components and/or procedures, deemed appropriate for the detection of explosives shall meet or exceed the following performance characteristics:

1. Detection of generally available types of high explosives (i.e., detonatable compositions) of U. S. or foreign manufacture including but not limited to compounds containing: Nitroglycerin, TNT (e.g., 40% dynamite).
2. The device or system provides high assurance of detection (probability of detection of at least 0.95) of high explosives (HE).
3. The minimum quantity of HE for which the required probability must be demonstrated must be no greater than 0.5 kg. The minimum quantity of HE must be detected with required probability when concealed on a person or in hand carried garments or packages.

CURRENTLY AVAILABLE EXPLOSIVE DETECTORS\*

<u>Model</u>	<u>Manufacture/Distributor</u>
EXD-2	Elscint, Inc. 138-160 Johnson Avenue P. O. Box 832 Hackensack, New Jersey 07602
Model-70	Ion Track Instruments, Inc. Three "A" Street Burlington, Massachusetts 01803

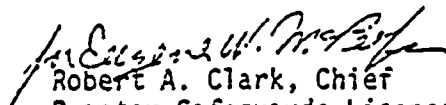
Reactor Safeguards Licensing Branch - 3 -

<u>Model</u>	<u>Manufacture/Distributor</u>
S-201 S-301	Leigh-Marsland Engineering, Ltd. 350 Weber Street, North Waterloo, Ontario, Canada N2J4E3  Contact: Security Products Marketing Office
Pye Dynamics	X-Ray Industrial Distributors, Inc. Representatives for Pye Dynamics 338 Delawanna Avenue Clifton, New Jersey 07014

\*These models have been tested by other agencies for detection of HE on personnel. Additional information may be found in Chapter 6 of Sandia "Entry Control Systems Handbook" SAND77-1033.

These models and others are acceptable if they meet or exceed the above Performance Requirements.

Review Guideline Number 20, dated April 10, 1978, is superseded by this revision.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors





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

MAY 26 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors, NRR

SUBJECT: ID BADGE - VITAL AREA ENCODING  
REVIEW GUIDELINE NUMBER 21

10 CFR 73.55(d)(7) states in part that: "The licensee shall positively control all points of personnel and vehicle access into vital areas. Access to vital areas shall be limited to individuals who are authorized access to vital equipment and who require access to perform their duties. Authorization for such individuals shall be provided by issuance of specially coded numbered badges indicating vital areas to which access is authorized." (Emphasis added.)

Many of the licensees plan to use automated/computer controlled access control systems to maintain positive access control to vital areas. This system uses a card or combination badge/key card which is encoded with a unique number. The access control computer is programmed to allow the individual holding this card access to specified vital areas. The program also correlates this unique card with one individual.

For licensees using an automated/computer access control system, an acceptable method of indicating the vital areas to which access is authorized is as follows:

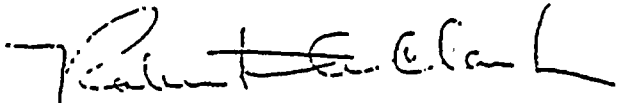
- \*(1) A numbered picture badge that indicates:
  - (a) employee or non-employee,
  - (b) access authorization level (protected area or protected and vital areas),
  - (c) escort requirements.
- \*(2) A key card that is uniquely numbered and is correlated to an individual.

\*The badge and key card may be the same article.



Reactor Safeguards Licensing Branch - 2 -

- (3) A record of each vital area to which the card, and thus the individual, is authorized access.
- (4) The key card is encoded to permit access to only those vital areas to which the individual has been granted access.



Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors, NRR







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

MAY 26 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch


FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors, NRR

SUBJECT: UNRESOLVED ISSUES - REVIEW GUIDELINE NUMBER 22

If, in the course of the review of the §73.55 security plan there arises, on a site specific basis, an issue that cannot be resolved in the discussions between the staff and the licensee, the review team leader will prepare a letter that will be sent to the licensee stating the requirement(s) that will be placed on the licensee in the Security Plan Evaluation Report (SPER) so that the security plan will meet the performance requirements of §73.55 and can be found acceptable by the staff. (e.g. "We will require the licensee to include the containment building area in his list of Vital Areas.") The requirement, so stated, will be incorporated into the Site Security Plan, as a condition for approval, when the SPER is issued.

Upon receipt of the letter of notification, the licensee may initiate the NRR appeal process through the licensing project manager if he finds the requirement unacceptable. If, upon completion of the appeal process the requirement has not been removed, the licensee may elect to incorporate the requirement into his Security Plan or to propose a compensating measure that will provide equivalent protection. In that event, a license amendment will be processed in accordance with §50.90 and §50.91 to identify the Security Plan, submitted by the licensee in compliance with §73.55, as the approved plan for the site and as a condition of the operating license.

In the event the licensee does not provide the required protection, the license amendment will be processed identifying the submitted Security Plan as the approved plan for the site and as a condition of the operating license. This is to be followed immediately with an Order for Modification of License, in accordance with 10 CFR 2.204, to incorporate the staff requirements into the license (i.e. the security plan).

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors, NRR





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

NOV 06 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch  
Division of Operating Reactors, NRR

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors, NRR

SUBJECT: PROTECTION OF NUCLEAR POWER PLANTS AGAINST INDUSTRIAL  
SABOTAGE BY THE INSIDER - REVIEW GUIDELINE #23

In order to meet the general performance requirements of §73.55(a), high assurance protection of a nuclear power plant against the threat of sabotage posed (1) with the active or passive assistance of an insider or (2) by an insider acting alone must be provided. Common to most scenarios that can be postulated for successful sabotage by a single insider, is the need for unrestricted access to vital areas and unrestricted time in these vital areas. Consequently, security measures that place controls on access to Vital I vital areas and/or limit the time allowed in Type I vital areas must be provided to meet the general performance objective of §73.55(a). We have encouraged licensees to develop security measures to achieve these objectives.

High assurance protection against sabotage by an insider may also be provided by security measures that permit unescorted access to Type I vital areas to only those individuals whose reliability and trustworthiness has been established using additional procedures that provide a high level of confidence.

The following measures, when properly applied in conjunction with those security measures implemented by the security plan to meet the requirements of §73.55 (b) through (h) provides an acceptable level of protection against sabotage by the insider.

General

A. Persons who are granted unescorted access to a Type II vital area (1) must have a need for access and (2) must have been found acceptable through a screening program described in ANSI N18.17-1973 Section 4.3 or the equivalent satisfactory employment record described in Review Guideline #1.

B. Persons who are granted access to a Type I vital area (1) must have a need for access, (2) must have been found acceptable through a screening program described in ANSI N18.17-1973 Section 4.3 (or Review Guideline #1),

\* Vital areas are discussed in Review Guideline #17



NOV 06 1978

and (3) must be authorized entry by the shift supervisor or other designated individual who has been informed of the estimated length of time to be spent in the Type I vital area. Authorization must be given on the shift the first entry is to be made and should terminate upon completion of the work. Extension of the authorization into the next shift can be made by the shift supervisor (or designated individual) informing his replacement for the next shift of the area, the work in progress and the personnel who have been authorized for entry.

C. Each of the following options when applied in conjunction with the provisions in (8) above provide acceptable levels of protection against sabotage by a single insider.

Option #1: Compartmentalization

The erection of barriers, installing doors, gratings or compartments to enclose vital equipment so that access to a single vital area cannot result in successful sabotage (i.e., eliminate Type I vital areas).

Option #2: Two-Man Rule

(a) Two or more individuals may be authorized to enter a Type I vital area together (1) if each person is advised of his responsibility to monitor the activities of his co-workers while in the area, (2) each individual is determined to have the knowledge and ability to identify unauthorized activities if conducted by his co-workers, (3) each individual must have the capability to observe, at any time and for as long as necessary to ascertain that activities are authorized, and (4) the capability to communicate with the control room or CAS/SAS must be available to each individual while in the Type I vital area.

OR

(b) Monitoring of the activities of one or several persons in certain Type I vital areas by an individual can be performed from a remote location (CCTV) providing the assigned individual has the knowledge and ability to identify unauthorized activities and can initiate a response to control and/or correct the situation.

Several examples are given below to illustrate the practical application of this procedure.

EXAMPLE:

Two men are both working on a task which requires that they be located within sight of one another; however, the task also requires that they do not normally



NOV 06 1979

- 3 -

face one another. The nature of the task does not prevent them from observing one another. This situation satisfies the above guidelines.

EXAMPLE:

Two men are both working on a task together. One man leaves the immediate area (but not the VA) to retrieve a part; he is out of eyesight for a few minutes. Nothing prevents his partner from following him to check on his whereabouts and nothing prevents the other man from returning at any time. This situation satisfies the above guidelines.

EXAMPLE:

Health physics personnel require knowledge of an individual's entrance into a VA and records time of entrance and work request authorizing. There is visual contact between HP and individual no less frequent than every 10 minutes and the capability for visual contact at any time. This satisfies the guideline.

Option #3: Personnel Reliability

The following may be permitted entry into Type I vital areas without escort or monitoring:

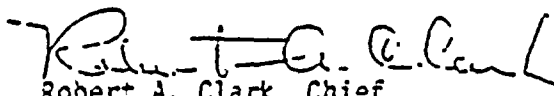
(a) An individual granted an NRC "Q" clearance;

OR

(b) An individual with (1) five years continuous service in a position that required access to a nuclear power plant Type I vital area; (2) certification by employer of trustworthiness and reliability based on observation of the employee during this service; and (3) a NRC sponsored NAC investigation (or its equivalent) has been completed with favorable results;

OR

(c) An individual with (1) a NRC granted operator license; (2) certification by employer of trustworthiness and reliability based on observation of the employee, and (3) a NRC sponsored NAC investigation or its equivalent has been completed with favorable results.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors, NRR





ATTACHMENT 2

SECURITY PLAN EVALUATION REPORT  
WORKBOOK

Revision 1

January 1978

## TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION.....	vi
CHAPTER 1 - SECURITY ORGANIZATION.....	1-1
1.1 MANAGEMENT ORGANIZATION.....	1-3
1.2 SECURITY ORGANIZATION.....	1-5
1.3 FACILITY PERSONNEL.....	1-7
1.3.1 Personnel Reliability.....	1-7
1.3.2 Personnel Training in Security Practices.....	1-10
1.4 PLANT SECURITY PERSONNEL.....	1-12
1.4.1 Qualifications for Employment in Security.....	1-12
1.4.2 Screening.....	1-14
1.4.3 Training.....	1-15
1.4.4 Retraining.....	1-17
1.4.5 Security Equipment.....	1-19
1.4.6 Authority of Guards to Use Weapons.....	1-22
1.4.7 Security Force Composition.....	1-23
1.5 LOCAL AND OTHER LAW ENFORCEMENT AGENCIES.....	1-25
1.6 ACCESS AUTHORIZATIONS.....	1-28
CHAPTER 2 - FACILITY AND ENVIRONS.....	2-1
2.1 GENERAL SITE AND AREA LAYOUT.....	2-1
2.2 FIXED AND MOBILE SECURITY POSTS IN THE OWNER- CONTROLLED AREA.....	2-1
2.3 EARLY WARNING DETECTION SYSTEMS.....	2-1
CHAPTER 3 - PROTECTED AREA PERIMETERS.....	3-1
3.1 PERIMETER BARRIER AND ISOLATION ZONE.....	3-1
3.1.1 Layout.....	3-1
3.1.2 Physical Barriers.....	3-3
3.1.3 Illumination and Surveillance.....	3-7
3.1.4 Intrusion Detection Hardware.....	3-10
3.1.5 Security Posts (Fixed and Mobile).....	3-14

## TABLE OF CONTENTS (Continued)

	<u>Page</u>
3.2 PROTECTED AREA PORTALS.....	3-16
3.2.1 Personnel Access Portals and Posts.....	3-16
3.2.1.1 Layout.....	3-16
3.2.1.2 Physical Structures.....	3-18
3.2.1.3 Locks, Keys, Combinations and Related Equipment.....	3-18
3.2.1.4 Security Posts.....	3-19
3.2.1.5 Search and Admittance Control Hardware.....	3-21
3.2.1.6 Picture Badge System.....	3-24
3.2.1.7 Communications.....	3-26
3.2.2 Vehicle and Cargo Access Portals And Posts.....	3-28
3.2.2.1 Layout.....	3-30
3.2.2.2 Physical Structures.....	3-32
3.2.2.3 Locks, Keys, Combinations and Related Equipment.....	3-32
3.2.2.4 Security Posts.....	3-33
3.2.2.5 Vehicle and Cargo Search Hardware.....	3-35
3.2.2.6 Communications.....	3-36
CHAPTER 4 - PROTECTED AREAS.....	4-1
4.1 LAYOUT.....	4-1
4.2 PHYSICAL STRUCTURES.....	4-3
4.3 ILLUMINATION AND SURVEILLANCE.....	4-4
4.4 SECURITY POSTS (FIXED AND MOBILE).....	4-6
4.5 ESCORTS.....	4-8
CHAPTER 5 - VITAL AREA BOUNDARIES.....	5-1
5.1 LAYOUT.....	5-4
5.2 PHYSICAL BARRIERS.....	5-5
5.2.1 Barrier Descriptions.....	5-5
5.2.2 Intrusion Detection Hardware.....	5-7
5.2.3 Control Room.....	5-11

## TABLE OF CONTENTS (Continued)

	<u>Page</u>
5.3 VITAL AREA PORTALS.....	5-13
5.3.1 Personnel Access Portals and Posts.....	5-13
5.3.1.1 Layout.....	5-13
5.3.1.2 Physical Structures.....	5-15
5.3.1.3 Locks, Keys, Combinations and Related Equipment.....	5-15
5.3.1.4 Security Posts.....	5-15
5.3.1.5 Access Control Hardware.....	5-16
5.3.1.6 Badge Control System.....	5-18
5.3.1.7 Communications.....	5-20
5.3.2 Vehicle Access Portals and Posts.....	5-22
5.3.2.1 Physical Structures.....	5-22
5.3.2.2 Security Posts.....	5-23
5.3.2.3 Communications.....	5-25
CHAPTER 6 - VITAL AREAS.....	6-1
6.1 CENTRAL ALARM STATION.....	6-1
6.1.1 Location and Layout.....	6-3
6.1.2 Physical Structures.....	6-5
6.1.3 Alarm and Surveillance Monitoring Hardware.....	6-7
6.1.4 Manning.....	6-10
6.1.5 Communications.....	6-12
6.2 SECONDARY ALARM STATIONS.....	6-14
6.3 OTHER VITAL AREAS.....	6-17
6.3.1 Surveillance Hardware.....	6-19
6.3.2 Security Posts (Fixed and Mobile).....	6-21
6.3.3 Escorts.....	6-23
CHAPTER 7 - CENTRAL COMMUNICATIONS SYSTEMS.....	7-1
7.1 TELEPHONE SYSTEM.....	7-1
7.2 INTERCOM AND PUBLIC ADDRESS SYSTEM.....	7-3
7.3 OTHER CENTRAL COMMUNICATIONS SYSTEMS.....	7-5

## TABLE OF CONTENTS (Continued)

	<u>Page</u>
CHAPTER 8 - RESPONSE TO SECURITY CONTINGENCIES.....	8-1
8.1 RESPONSE FORCE AVAILABILITY.....	8-1
8.2 ASSIGNMENT OF RESPONSIBILITIES.....	8-3
CHAPTER 9 - SPECIAL SECURITY MEASURES DURING REFUELING/MAJOR MAINTENANCE OPERATIONS.....	9-1
CHAPTER 10 - SECURITY MEASURES DURING CONSTRUCTION OPERATIONS.....	10-1
CHAPTER 11 - OVERALL PHYSICAL SECURITY PROGRAM PERFORMANCE.....	11-1
CHAPTER 12 - TESTS, INSPECTIONS AND MAINTENANCE.....	12-1
12.1 PHYSICAL BARRIERS AND ACCESS POINTS.....	12-1
12.2 ALARMS, ANNUNCIATORS AND SURVEILLANCE SYSTEMS.....	12-3
12.3 SPECIAL PURPOSE DETECTORS.....	12-5
12.4 COMMUNICATIONS EQUIPMENT.....	12-7
12.5 SECURITY PERSONNEL EQUIPMENT.....	12-9
CHAPTER 13 - SECURITY RECORDS.....	13-1
13.1 SECURITY TOURS, INSPECTIONS AND TESTS.....	13-3
13.2 MAINTENANCE.....	13-5
13.3 ALARM ANNUNCIATIONS.....	13-7
13.4 SECURITY RESPONSE.....	13-9
13.5 AUTHORIZED INDIVIDUALS.....	13-11
13.6 ACCESS TO VITAL AREAS.....	13-13
13.7 EMPLOYEE ACCESS.....	13-15
13.8 NONEMPLOYEE ACCESS.....	13-17
CHAPTER 14 - SECURITY AUDITS.....	14-1
14.1 PROGRAM AUDITS.....	14-1

## APPENDICES

A - Contingencies and Supporting Discussion Requirements.....	A-1
A - NRR Supplemental Staff Position on Personnel Search Requirements.....	B-1
C - Review Guidelines.....	C-1

## INTRODUCTION

The Security Plan Evaluation Report (SPER) Workbook has been developed to provide (1) an aid to the evaluation of Licensee/Applicant Physical Security Plans, and (2) the single source for preparing the SPER. Using the workbook will help provide for a consistent evaluation of all physical security plans. The workbook is organized into the same chapters and sections as NUREG-0220, "Interim Acceptance Criteria for a Physical Security Plan for Nuclear Power Plants," for ease in correlating between the two.

Each section is organized into the following subsections:

Acceptance Criterion - The statement used as the basis for making a judgment concerning the achievement of a security measure specified by 10 CFR Part 73.55.

Source - The section of the regulation used for justification of the acceptance criterion is provided. When an explanation is required for clarification, it is also provided.

Objective - A statement of the goal to be achieved by satisfying the requirement specified in 10 CFR Part 73.55.

### Review Procedures:

Security Plan Review - Information which the reviewer looks for as he examines the Physical Security Plan. The information is that which is needed to evaluate the plan against the acceptance criterion. Review Guidelines to aid in the evaluation of the plan are provided as Appendix C.

Site Visit - Record of team members' observations from visit to reactor site.

Additional Review - Additional review to be made by the review team before a decision is to be made as to whether the Physical Security Plan is satisfactory or not. The type of review and documentation to be reviewed should be stated.

Evaluation Findings - A positive statement specifying how the plan either satisfactorily or unsatisfactorily meets the requirements of the applicable acceptance criterion is to be made by the reviewer. If the statement is of an unsatisfactory nature, then the reviewer must make remarks addressing one of the following: (1) if the acceptance criterion must be met before the plan will be acceptable, then he must be explicit in specifying what is required before this criterion will be acceptable; and (2) if the acceptance criterion

does not have to be satisfied because it is compensated for elsewhere, then he must explicitly state what the compensation is and where it is in the plan. The reviewer should also state the impact of this on the Chapter 11 acceptance criterion, "overall physical security program performance." A model statement with provisions for terms to be struck out or added is provided. The model statement, if appropriate, is intended to be lifted from the workbook for inclusion into the SPER. The reviewer does not have to make additional comments if he feels the model statement is satisfactory as written.

The workbook, when completely filled in, will also provide a record of the justification for accepting or rejecting a plan. This record may prove useful should any future discrepancies occur as a result of I&E inspections.





## CHAPTER 1 - SECURITY ORGANIZATION

Acceptance Criterion 1.A: The licensee shall establish a security organization, including guards, to protect his facility against industrial sabotage.

Source: 73.55(b)(1)

Objective: Assure that a security force is onsite to provide continuous protection against industrial sabotage.

Review Procedures:

Security Plan Review:

Assure there is a specific organization with personnel continuously onsite with responsibility for protection against industrial sabotage. Confirm this organization does not have any other responsibilities that would conflict with the responsibility to protect against industrial sabotage. Identify the person responsible for day-to-day administration of the security organization.

Assure that the security organization includes guards. Identify other personnel such as watchmen and armed response individuals, if they are included in security organization.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

To protect against industrial sabotage, the licensee has established a security organization administered by the \_\_\_\_\_ and including guards, watchmen and armed response individuals who are employees of (the licensee, a contractor to the licensee). This organization has no other responsibilities which would interfere with providing the required level of physical security.

## 1.1 MANAGEMENT ORGANIZATION

Acceptance Criterion 1.1.A: Management of the physical security organization shall be independent of the management of the operating organization.

Source: 73.55(a) [Staff requirement based upon need for high assurance protection against a design basis threat which includes an insider in any position].

Objectives: To assure appropriate resolution of conflicts between operations and security in day-to-day activities. To assure the security organization has means of appeal.

Review Procedures:

Security Plan Review:

Identify the highest ranking individual onsite with responsibilities solely in security.

Identify the lowest managerial level with responsibility for both operations and security. Review job description of this managerial level. Confirm this individual is high enough in the organization to maintain the required level of physical security while meeting operational demands.

Identify the corporate office to which the onsite security organization reports. Confirm this is an appropriate path for appeal.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The \_\_\_\_\_ is the highest ranking onsite manager with responsibilities solely in security. He reports to \_\_\_\_\_, which is the lowest level of management which is responsible for both operations and security. This level of management is appropriate for maintaining the required level of physical security while meeting operational demands. The onsite security organization reports to \_\_\_\_\_ in the licensee's corporate management, thus providing an appropriate path of appeal.

## 1.2 SECURITY ORGANIZATION

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.

Source: 73.55(b)(2)

73.55(a) [Staff requirement based upon need for effective operations/security coordination to assure high assurance protection].

Objective: To assure appropriate direction of physical security, particularly during contingencies. To assure effective coordination between security and plant operations at all times.

Acceptance Criterion 1.2.B: A clear chain of succession of responsibility shall be established for the transfer of authority, in the event of disablement of a key member of the physical security organization, during an incident.

Source: 73.55(b)(2), 73.55(a) [Staff requirement based upon need for continuous effective coordination of the physical security organization during incidents involving use of force].

Objective: Assure continuous effective direction of physical security force.

Review Procedures:

Security Plan Review:

- A) Review the chain of command of the security organization. Identify (by position) the members of the security organization who direct the security activities for each shift. Identify (by position) the individual in charge of all operations at the site. Verify that procedures for communication (without involvement of off-duty superiors) exist between these two individuals.

The individual in charge should not have routine assignments, such as manning CAS, SAS, etc., but must have time to direct all activities of the security organization during an incident.

- B) Confirm that a chain of succession exists through all levels of the security organizations..

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The \_\_\_\_\_ is onsite at all times and has the authority to direct the physical security organization in meeting the threat. He also has the authority to seek local law enforcement support if, in his judgment, it is required.

A clear succession of responsibility has been established. In the event of the disablement of the \_\_\_\_\_, he will be replaced by \_\_\_\_\_. Subsequent succession will be in the following order: \_\_\_\_\_.

### 1.3 FACILITY PERSONNEL

#### 1.3.1 Personnel Reliability

Acceptance Criterion 1.3.1.A: The licensee shall develop and conduct a screening program for all personnel who are authorized for unescorted access to the protected area. As a minimum, this program shall follow the employee screening guidance in American National Standard ANSI N18.17, "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 shall be treated as employees. A contractor screening program is acceptable if it can be shown that the program provides coverage equivalent to or greater than ANSI N18.17.

Source: Statement of Considerations for 73.55  
73.55(a) [Staff requirement based upon need for high assurance protection against insider].

Objective: Reduce the likelihood of sabotage participation by persons granted unescorted access.

Acceptance Criterion 1.3.1.8: Evidence of completed employee screening shall be maintained on all employees granted unescorted access to the protected area, and shall be available for USNRC inspection.

Source: 10 CFR Part 19

Objective: Assure that Inspection and Enforcement personnel will be permitted access to records which demonstrate that specified licensee procedures for employee screening are being carried out. Note that I&E need not be permitted access to information obtained by these procedures.

Review Procedures:

Security Plan Review:

- A) Confirm that the screening program is at least equivalent to ANSI 18.17. An equivalent program should include a preemployment investigation for adverse character traits, a preassignment examination to identify aberrant behavior, and continued observation during assignment for indications of aberrant behavior. Particular emphasis should be given to contractor personnel. The burden of verifying the adequacy of contractor screening programs rests with the licensee (applicant). An unverified statement by the contractor that he provide equivalent screening is not acceptable. The licensee (applicant) must provide a description of the screening procedures used, including descriptions of accepted contractors' screening procedures.

Where state and/or local law limits the extent of preemployment screening, compensatory measures must be proposed by the licensee (applicant) to provide equivalent protection against the insider. An example of such a "compensatory measure" would be employment in a nonsensitive position (e.g., at a fossil plant) coupled with close observation and/or monitoring of performance prior to assignment at the nuclear plant site.

- B) Confirm that the physical security plan commits to maintaining records showing that procedures established for authorized employee screening have been completed and that these records will be available for NRC inspection.

Questions and Comments:



Site Visit:

Additional Review:

Evaluation Findings:

The licensee will conduct a screening program for all personnel granted unescorted access to the protected area which, as specified in ANSI N18.17, include an investigation to detect adverse character traits, an examination to identify aberrant behavior, and continued observation for indications of aberrant behavior.

The licensee has stated that records documenting completion of screening procedures will be maintained for all employees granted unescorted access to the protected area and that they will be available for NRC inspection.

### 1.3.2 Personnel Training in Security Practices

Acceptance Criterion 1.3.2.A: The licensee shall implement a training program to assure that all individuals authorized for unescorted access to the protected area (other than physical security force personnel) understand their role in physical security and their responsibility in the event of security incidents.

Source: 73.55(a) [Staff requirement based upon need for high assurance protection against design basis threat].

Objective: Assure that all authorized personnel understand the sabotage threat and their duties in deterring, detecting and neutralizing this threat.

Review Procedures:

Security Plan Review:

Confirm that the training program is required for all nonsecurity force personnel authorized unescorted access to the protected area.

Confirm that the training program covers the threat of sabotage and responsibilities in deterring, detecting and neutralizing it.

Confirm that documentation of completed employee training will be maintained.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

A satisfactory program for security training of authorized individuals is described in the \_\_\_\_\_. This program encompasses training in \_\_\_\_\_, \_\_\_\_\_ and \_\_\_\_\_ for a total of \_\_\_\_\_ hours. All employees will be so trained and a certification of training will be provided by the instructor.

## 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) shall possess physical and mental capabilities consistent with their role in the detection, assessment and neutralization of security contingencies. These qualifications must be checked at least once each 12 months.

Source: 73.55(b)(4)

Objective: Assure that personnel assigned to the physical security force possess the appropriate physical and mental capabilities.

#### Review Procedures:

Review the qualifications of security organization employees. The physical qualification of guards, watchmen and armed response individuals should include criteria for height, weight, sight, hearing, etc. Psychological evaluations should be given to all security organization employees.

Regulatory Guide 5.20 identifies an acceptable set of qualifications.

#### Questions and Comments:

D

Site Visit:

Additional Review:

Evaluation Findings:

The licensee (applicant) has established a set of minimum physical and mental qualifications for security personnel to assure an appropriately qualified security force, capable of meeting all security contingencies.

#### 1.4.2 Screening

There are no additional criteria.

### 1.4.3 Training

Acceptance Criterion 1.4.3.A: All members of the physical security organization shall receive training consistent with their roles.

Source: 73.55(b)(4)

Objective: Assure that all physical security employees have the knowledge required for the performance of their job functions.

Review Procedures:

Security Plan Review:

Review the training program for members of the physical security force, including the curriculum, criteria for successful completion, firearms qualification (for guards and armed response individuals), and the interval between retraining and requalification. Regulatory Guide 5.20 provides an acceptable training program.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

All members of the physical security organization will receive training consistent with their roles in a program which follows Regulatory Guide 5.20.



#### 1.4.4 Retraining

Acceptance Criterion 1.4.4.A: Each guard, watchman and armed response individual shall be requalified according to Regulatory Guide 5.20. Such requalification shall be documented.

Source: 73.55(b)(4)

Objective: Assure that all physical security force personnel possess the appropriate physical and mental capabilities throughout their assignment to the force.

Review Procedures:

Security Plan Review:

Confirm that the security plan contains provisions for guard, watchman and armed response individual annual refresher training to include responsibilities of the security organization and security procedures during normal and contingency situations.

Confirm that the security plan provides for weapon requalification at least once each 12 months.

Confirm that the results of the refresher training are to be documented.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The licensee will establish an annual requalification program, for all guards, watchmen and armed response individuals, which satisfies the requirements of Regulatory Guide 5.20. Documentation of successful requalification will be provided.

#### 1.4.5 Security Equipment

Acceptance Criterion 1.4.5.A: All guards shall wear uniforms. These uniforms should allow guards to be clearly distinguishable from local law enforcement and other onsite personnel.

Source: 10 CFR Part 73.2

Objective: To assure that guards are clearly distinguishable from local law enforcement and other onsite personnel, particularly during security incidents.

Acceptance Criterion 1.4.5.B: The guards and armed response individuals shall be provided with weapons (including shotguns or rifles) and equipment consistent with the requirements of Federal and local laws and the strategy for meeting the threat at this facility.

Source: 73.55(h)(3), 73.55(a) [Shotguns or rifles is staff requirement on weapons to meet the threat].

Objective: Assure that licensee's weapon selection is suitable for the site and that guards and armed response personnel have sufficient weaponry to neutralize the design basis industrial sabotage threat.

Acceptance Criterion 1.4.5.C: All on-duty physical security force personnel must be capable of continuous communication with the the central and secondary alarm stations when within the owner-controlled area. They should also be capable of direct communication with all other members of the security force who are also in owner-controlled area.

Source: 73.55(f)(1) [Specified communication range is staff requirement based upon the need to provide high assurance protection. Direct communication is recommended since it allows security force director to directly communicate with personnel during incident response].

Objective: Assure security personnel ability to provide warning and receive direction during incident response.

Review Procedure:

Security Plan Review:

- A) Review the uniforms and equipment supplied to the guard force. Ascertain that the recommendations of Regulatory Guide 5.20 are met or exceeded.
- B) All guards and armed response individuals must be armed consistent with the threat defined in §73.55(a). This requires at a minimum a .38 cal. revolver to be worn at all times (including

during patrols within a vital area), and the immediate availability of 12 gauge shotguns or rifles for each armed response.

- C) Continuous communication with CAS and SAS requires two-way (single channel) radio in most situations. Hard-wired intercom, or equivalent, may be acceptable continuous communication for certain immobile posts, such as a defensive position or gatehouse. Confirm that there are no areas where communication between portable radios and the central alarm station and secondary alarm station is not possible.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Guard uniforms are designed to clearly distinguish the wearer from local law enforcement and other onsite personnel. Watchmen and armed response personnel wear the same uniforms.

Guards and armed response personnel are provided the following equipment for use in day-to-day operations: \_\_\_\_\_. The following additional equipment is available for contingencies: \_\_\_\_\_. This provision of equipment is consistent with the requirements of Federal and local laws and the facility's strategy for meeting the threat.

While on duty in the owner-controlled area, all guards and watchmen will carry portable radios which are capable of continuous communication with the central and secondary alarm stations. There are no areas in which effective radio transmission to all points in the owner controlled area is not possible.

#### 1.4.6 Authority of Guards to Use Weapons

There are no specific criteria.

#### 1.4.7 Security Force Composition

Acceptance Criterion 1.4.7.A: There shall be a nominal response force of ten guards and armed response individuals. This number shall include at least five guards.

Source: 73.55(h)(2)

Objective: Assure that the response force is of adequate size to provide assessment and neutralization capability consistent with meeting the requirement for high assurance protection against industrial sabotage.

Review Procedure:

Security Plan Review:

Determine the minimum number of armed response personnel per shift. Verify that the response force includes at least five guards. If the response force includes armed response individuals (other than guards), verify that proper justification is provided in Section 8. If the armed response force is less than ten, determine what additional features of the security system are provided to justify the reduction in the response force. Compare these additional features against the list of factors influencing response force size in the statement of consideration to the revision of 10 CFR Part 73 (Federal Register, February 24, 1977). For each of the factors quoted as justification, compare the licensee's (applicant's) provision to the acceptance criteria for that portion of the security system to determine the additional features constitute a significant improvement in overall security, or enhance the effectiveness of the guard force sufficiently to warrant the reduction in the armed response force.

Verify that a sufficient number of security force personnel will be available to provide for continuous occupation of the CAS and SAS in addition to the required size of the armed response force. (Note that personnel performing search and/or access control functions may leave their posts during a mobilization of the response force, provided that any portals are locked and alarmed.)

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The security organization includes an armed response force composed of (at least five) uniformed armed guards and armed response personnel. The compatibility of job functions of the armed response individuals is discussed in Chapter 8 of this report. We have evaluated the additional features of the security system proposed in lieu of a larger response force. These additional features include (... description...). We conclude that the overall effectiveness of the security system with these additional features and a response force of \_\_\_\_\_ is acceptable.



## 1.5 LOCAL AND OTHER LAW ENFORCEMENT AGENCIES

Acceptance Criterion 1.5.A: Documentation shall be presented that demonstrates 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.

Source: 73.55(a) [Staff requirement based upon need to assure that there is a firm commitment to the level of local law enforcement support taken credit for in the plan].

Objective: Assure that the commitment of law enforcement support is documented.

Acceptance Criterion 1.5.B: Written agreements shall 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.

Source: 73.55(a) [Staff requirement based upon need to assure that high assurance protection is not undermined by conflicts of authority in contingency situations].

Objective: Assure that there is no conflict of authority in the management of a contingency situation requiring support of outside agencies.

Acceptance Criterion 1.5.C: Documentation shall be presented demonstrating 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 facility.

Source: 73.55(a) [Staff requirement based upon need to assure that supporting agencies have the knowledge required to fulfill their roles in providing high assurance protection].

Objective: Assure that local law enforcement personnel have sufficient knowledge to permit effective participation in contingency response.

Review Procedures:

Security Plan Review:

- A) Verify the existence of letters from all local and other law enforcement agencies which commit them to supporting the facility during security incidents. The letters should state the level of support to be provided.

- B) Verify the existence of written agreements between the plant and law enforcement agencies which identify and acknowledge:
  - 1) The organization with the authority to direct the response onsite.
  - 2) The position of authority within the organization.
  - 3) The authority to direct response within the company-owned property will be directed by a single individual.
- C) Confirm that a commitment to familiarize appropriate law enforcement agency personnel with the facility includes:
  - 1) Periodic plant tours.
  - 2) Periodic briefings to include security organization, responsible individuals, response procedures, and special constraints imposed on security in protecting a nuclear facility.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The plan includes letters from all supporting local law enforcement agencies documenting the level of support they will provide. These letters verify the level of support taken credit for in the plan.

The plan includes written agreements from all supporting local law enforcement and other protection agencies documenting that direction of security operations will always rest with a single individual. Authority for direction will be held as follows: \_\_\_\_\_.

The licensee has described the familiarization program provided supporting protective agencies and has certified that this program has been completed by the following key personnel: \_\_\_\_\_. This program will be held each year and covers response procedures, plant layout and constraints in protecting a nuclear facility.

## 1.6 ACCESS AUTHORIZATIONS

Acceptance Criterion 1.6.A: Criteria for granting escorted or unescorted protected area access to personnel and vehicles shall be established and documented. These criteria shall provide the means for clearly establishing the need for access.

Source: 73.55(4), (5)  
73.55(a) [The requirement for establishing a clear need for access is based upon the staff's position that strict limitation of the number of personnel and vehicles granted access is an essential element in providing high assurance protection].

Objective: To assure that a clear policy exists for granting protected area access to personnel and vehicles. To assure that the number granted access is strictly limited.

Acceptance Criterion 1.6.B: Identification and authorization criteria for accepting packages and material for delivery into the protected area shall be established.

Source: 73.55(b)(3)

Objective: Assure that definitive criteria are established for accepting packages and material for delivery into the protected area.

Review Procedures:

Security Plan Review:

Review the licensee's (applicant's) procedures for:

- A) Permitting escorted access to the protected area. Particular attention should be given to visitor identification, verification of identity, affiliation, clearance, etc.

Updating the list of authorization for unescorted access to the protected area. A specific justification of the need for this authorization must be part of this procedure.

- B) Checking that packages and other materials for delivery into the protected area are expected.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The licensee has established procedures which document a satisfactory set of criteria for protected area access. Criteria for granting personnel and vehicle access can be summarized as follows: \_\_\_\_\_  
These criteria require a clear need for personnel and vehicle access.

The licensee has established definitive identification and authorization criteria for accepting packages and material for delivery into the protected area. These criteria are as follows:



## CHAPTER 2 - FACILITY AND 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

There are no specific acceptance criteria.





## CHAPTER 3 - PROTECTED AREA PERIMETER

### 3.1 PERIMETER BARRIER AND ISOLATION ZONE

#### 3.1.1 Layout

Acceptance Criterion 3.1.A: Isolation zones shall be maintained in outdoor areas adjacent to the physical barrier at the perimeter of the protected area. These isolation zones shall extend at least 20 feet on each side of the perimeter and must be free of visual obstructions to permit accurate assessment of security incidents detected on either side of the protected area perimeter barrier.

Source: 73.55(c)(3) [Extent of isolation zone is staff requirement in order to allow time for accurate assessment and to prevent bridging of intrusion detection systems].

Objective: Provide an area free from visual obstruction.

Review Procedures:

Security Plan Review:

Examine drawings of the facility layout to confirm the existence of:

- 1) A physical barrier at the perimeter of the protected area.
- 2) An isolation zone, free from obstructions, extending 20 feet on both sides of the protected area barrier. All items located in the isolation zone must be identified.
- 3) Parking facilities beyond the isolation zone.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The perimeter barrier which encompasses the protected area includes an isolation zone (cleared area) extending 20 feet on each side of the perimeter. This isolation zone permits unimpeded visual examination of the perimeter barrier, aids in the prevention of concealed circumvention of the barrier, and facilitates immediate visual assessment in case of an intrusion detection.

### 3.1.2 Physical Barriers

Acceptance Criterion 3.1.2.A: Physical barriers at the protected area perimeter shall at the minimum satisfy the requirements of 10 CFR Part 73.2(f)(1), (2).

Source: 73.2(g)

Objective: Assure that fences and walls forming the protected area barrier satisfy regulatory requirements.

Acceptance Criterion 3.1.2.B: All security keys, locks, combinations and related equipment used to control access to protected and vital areas shall be controlled to reduce the probability of compromise. 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. All security locks shall satisfy the criteria stated in 10 CFR Part 73.2(m). All security locks, keys, combinations and related equipment shall satisfy the requirements of Regulatory Guide 5.12 except that cipher locks are not needed for vital area entry. All security keys and locks shall be kept in a locked cabinet when not in use.

Source: 73.55(d)(9), 73.2(m)

Objective: Minimize the likelihood of compromise of keys, locks, combinations and other related equipment.

Acceptance Criterion 3.1.2.C: Measures shall be taken to fully compensate for any reduction in the effectiveness of a physical barrier at the protected area perimeter.

Source: 73.55(g)(1)

Objective: Assure that the level of sabotage protection is not degraded by a reduction in the effectiveness of a physical barrier.

Review Procedure:

Security Plan Review:

- A) Confirm a commitment to a protected area barrier that provides penetration resistance at least equal to that of 11 AWG chain link fence with wire mesh at least seven feet in height topped with at least a one-foot top guard of barbed wire (at least four standards 3" apart) angled outward from the vital areas between 30 and 45 degrees from the vertical. The ground under the fence should be of such consistency as to prevent undetected

access. Bottoms of fences must be secured in a fashion that will prevent "undetected penetration." Confirm that the sides of buildings or walls which constitute part of the barrier be at least eight feet in height and have a barbed wire topping as described above. Building sides and walls constructed of nonscalable facades and 18 feet or greater in height need not have a top guard. Culverts, ditches and other penetrations through the protected perimeter should be designed to provide penetration resistance equal to the overall barrier.

- 8) Confirm the existence of combination, key and lock control procedures to include the following:
- 1) Combinations of locks or padlocks used to secure gates or doors into protected and vital area perimeters, and for access to vital equipment, should be known only to those authorized access to the material or to the area. They should be changed when repositories or areas are first placed in use, whenever a person knowing the combination no longer requires it as a result of reassignment of duties or termination, whenever the combination may have been compromised, or at least twice every year. A record of the combinations of locks should be kept in a location that is secured by a combination lock.
  - 2) Keys and cards to locks or padlocks used to secure gates or doors to protected and vital area perimeters should be issued only to persons authorized access to the material or to the area. Keys or cards in use should be checked in at the end of each shift or workday, and a log should be maintained showing keys and cards, users, in and out times, and other pertinent information. Keys and cards should be recovered from reassigned personnel or cores replaced and an inventory conducted whenever: (1) a core, key, or card is lost or missing, (2) the lock core, key or card has been compromised, or (3) unrecorded keys or cards are found. In a mastered system, a complete remastering of the system should be conducted whenever a core, card, master or control key, or a lock is lost or compromised.
  - 3) A record of all locks, cores, keys and cards should be maintained and kept in a location secured by a combination lock. A physical inventory of locks, cores, keys and cards (used for protection of facilities) should be conducted semiannually. Unused locks, cores, keys and cards should be stored in a location secured by a combination lock. A specific individual at each site should be named and placed in charge of all locks, cores, keys and cards.

- 4) Confirm that all security locks, keys, combinations and related equipment will satisfy the requirements of Regulatory Guide 5.12.
- C) Confirm the existence of specified compensatory measures to be used should there be a reduction in the effectiveness of a physical barrier. Applicable compensatory measures include:
  - 1) Additional guards.
  - 2) Barrier replacement segments onsite.
  - 3) Additional surveillance, detection and alarm systems available for rapid installation.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The protected area perimeter barrier is composed of fences constructed of \_\_\_\_\_ topped by three strands of barbed wire on brackets angled outward at \_\_\_\_\_ degrees from the vertical with an overall height of eight feet, including the barbed topping.

All security keys, locks, combinations and related equipment to which an employee had access will be changed upon termination of that employee with the company and will be controlled using the following measures: \_\_\_\_\_ All security locks will satisfy the requirements of 10 CFR Part 73.2(m). All security locks, keys, combinations and related equipment will satisfy the requirements of Regulatory Guide 5.12.

The following measures have been judged satisfactory to fully compensate for any reduction in the effectiveness of the protected area barrier:

---

### 3.1.3 Illumination and Surveillance

Acceptance Criterion 3.1.3.A: Illumination shall be maintained at the protected area perimeter including the isolation zones. The minimum level of illumination is 0.2 footcandle measured horizontally at ground level.

Source: 73.55(c)(5)

Objective: Assure that sufficient light is available to permit accurate assessments using the naked eye.

Acceptance Criterion 3.1.3.B: 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.

Source: 73.55(b)(4), 73.55(h)(4)

Objective: Assure accurate assessment of security incidents at the protected area perimeter or in adjacent isolation zones.

Acceptance Criterion 3.1.3.C: Capability shall be provided for transmission of equivalent surveillance data to the central and secondary alarm stations.

Source: 73.55(a) [Staff interpretation of requirement for protection against insider assisting external threat].

Objective: Assure that an insider with surveillance responsibility cannot assist an external adversary by not correctly reporting detection or assessment information.

Review Procedures:

Security Plan Review:

- A) Confirm a commitment to the required illumination and compensatory measures for loss of illumination beyond one minute.
- B) Confirm that a surveillance system with a field of view of the entire isolation zone is specified.

If the identified system is electronic, confirm that both the CAS and SAS have monitoring devices.

If the identified system relies on guards, confirm that a guard's position remains in the field of view of another guard.

- C) Confirm that simultaneous monitoring of the surveillance system is specified for both the central and secondary alarm stations.

Questions and Comments:



Site Visit:

Additional Review:

Evaluation Findings:

Illumination at the protected area perimeter including the isolation zone will be maintained at a minimum level of 0.2 footcandle measured horizontally at ground level.

A CCTV system will be employed which will provide the capability of observing unauthorized activities in the isolation zone and accurately assessing intrusion detections made at the protected area perimeter. The system will employ \_\_\_\_\_ cameras and \_\_\_\_\_ monitors which will be located in the CAS. After a detection the image of the camera observing that zone is displayed.

A satisfactory CCTV system will be employed to show, in both the CAS and SAS, the image of the zone in which a detection occurs.

### 3.1.4 Intrusion Detection Hardware

Acceptance Criterion 3.1.4.A: The intrusion detection system shall provide high assurance detection of all penetrations of the protected area perimeter. All detection systems hardware shall satisfy the criteria of Regulatory Guide 5.44 or equivalent.

Source: 73.55(a) [Staff requirement based upon need to provide high assurance protection].

Objective: Assure that high assurance detection is provided at the protected area perimeter and that the effectiveness of this detection is not degraded by false and nuisance alarms.

Acceptance Criterion 3.1.4.B: All intrusion alarm systems shall be provided with emergency electrical power as stated in Regulatory Guide 5.44. This power shall be provided from a source within the protected area.

Source: 73.55(e)(2)

Objective: Assure that intrusion alarm systems continue to function normally in the event of a loss of offsite power.

Acceptance Criterion 3.1.4.C: All intrusion alarm systems shall have a frequency of false and nuisance alarms such that the response capability is not degraded. The intrusion alarms should satisfy the frequency of false and nuisance alarms specified in Regulatory Guide 5.44.

Source: 73.55(a) [Staff interpretation of requirement to achieve high assurance detection].

Objective: Assure that the frequency of false and nuisance alarms does not degrade the response capability.

Acceptance Criterion 3.1.4.D: All intrusion detection systems shall 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. These systems shall satisfy the tamper-indicating and self-checking requirements of Regulatory Guide 5.44.

Source: 73.55(e)(2)

Objective: Assure that the effectiveness of the intrusion detection system cannot be intentionally degraded for more than one minute without compensation if the cause is system failure.

Acceptance Criterion 3.1.4.E: All intrusion detection system hardware must annunciate at the central and secondary alarm stations. The annunciation of an alarm shall indicate the type of alarm (e.g., intrusion alarm, emergency exit alarm, etc.) and location.

Source: 73.55(e)(1), 73.55(e)(2)

Objective: Assure that an insider cannot prevent response by ignoring an alarm and that the response can be made appropriate to the type of alarm received.

Acceptance Criterion 3.1.4.F: Compensatory measures shall be established and employed to assure an equivalent level of protection in the event of detection hardware outage.

Source: 73.55(g)(1)

Objective: Assure that intrusion detection performance is not degraded by a failure of detection hardware.

Review Procedures:

Security Plan Review:

- A) Confirm that an intrusion detection system is specified for the perimeter of the protected area and that it is capable of detecting 95 out of 100 intruders who are running, walking, crawling, rolling or jumping.
- B) Confirm that the intrusion detection system includes the following emergency power capability:
  - 1) An automatic switch over from primary power to emergency battery and generator or emergency battery power without causing an alarm, but there is an indication.
  - 2) Twenty-four hour operation without recharging batteries or refueling generators, unless fuel is onsite.
- C) Confirm that the intrusion detection system performance includes the following average false alarm and nuisance alarm specifications:
  - 1) False alarm rate not to be greater than one per week per zone.
  - 2) Nuisance alarm rate not to be greater than one per week per zone.

- 3) False alarm and nuisance alarm rate not to be greater than one per day per zone under continuous visual observation.
- D) Confirm that intrusion detection system description includes the following tamper-indicating/self-checking capability:
- 1) All enclosures are equipped with tamper switches or trigger mechanisms compatible with alarm switches.
  - 2) Trigger mechanism/tamper switches remain in operation when system is in ACCESS mode.
  - 3) Controls that affect sensitivity of alarm system are located within tamper-resistant enclosure.
  - 4) Signal lines connecting alarm relays with alarm monitors are supervised.
  - 5) Signal line connecting sensor electronics with processing electronics is supervised.
- E) Confirm that the intrusion detection system description includes the following alarm capability.
- 1) Annunciates in both the central and secondary alarm stations.
  - 2) Detection of an intruder.
  - 3) Failure of emergency power to properly operate the system in the event of primary power loss.
  - 4) Indication of tampering.
  - 5) Failure of aging components which cause system failure.
  - 6) The type of alarm annunciation shall indicate the type of problem (detection, power failure, tampering, system failure).
- F) Confirm that procedures are documented, which include the posting of guards/watchmen to provide visual coverage in the zone(s) with the hardware outage.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

An intrusion detection system will be installed which will detect an intruder in the secured zone 95 out of 100 times. The system will detect the following modes of intruder penetration: running, walking, crawling, rolling and jumping.

The intrusion alarm system at the protected area perimeter will be provided with an onsite source of emergency power. This power system meets the requirements of Regulatory Guide 5.44 in that: switch over is automatic, there is indication of switch over but no alarm, and it is capable of sustaining operation for a minimum of 24 hours.

The intrusion alarm system will be installed to provide, on the average, no more than one false and one nuisance alarm per zone per week, thus meeting the requirements of Regulatory Guide 5.44.

The intrusion alarm system will satisfy the tamper-indicating and self-checking requirements of Regulatory Guide 5.44. All equipment enclosures and sensitivity controls will be equipped with tamper switches or triggering mechanisms which operate even when the system is in the ACCESS mode. All signal lines connecting alarm relays with alarm monitors are supervised. The system will be self-checking.

All intrusion detection system hardware will annunciate at both the central and secondary alarm stations and will indicate the type and location of the alarm.

Compensatory measures have been established and will be employed to provide an equivalent level of protection in the event of intrusion detection hardware outage. In the event of failure in a single zone, a single guard or watchman will be posted to continuously observe the affected zone. In the event of a total system failure, guards or watchmen will be posted to observe all of the protected area boundary.

### 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 should be bullet-resistant. A structure should be judged bullet-resistant if it satisfies the requirements of 10 CFR Part 73.2(s), Underwriter's Laboratories High Power Rifle Rating. All entrance points to these structures should be locked when occupied.

Source: 73.55(a) [Staff recommendation based upon need for high assurance protection].

Objective: Establish requirements for defensive positions which are mentioned in the statement of considerations.

Acceptance Criterion 3.1.5.B: The protected area perimeter barrier and adjacent isolation zones shall be patrolled at random times and on random paths with the same frequency (at least once in every two hours) as the patrol of exterior areas (See Acceptance Criterion 4.4.B). Checks of the exterior areas within the protected area and the protected area perimeter barrier and adjacent isolation zones may be accomplished on the same patrol.

Source: 73.55(c)(4)

Objective: Assure that the protected area perimeter barrier and adjacent isolation zones receive frequent close visual inspection at unpredictable times to detect abnormal occurrences.

Review Procedures:

Security Plan Review:

- A) Confirm that any specified defensive positions established at the protected area barrier include a bullet-resistant specification.
- B) Confirm a commitment for security patrols of the protected barrier and adjacent isolation zones at least once every two hours. Patrols may not be necessary if defensive positions are established and have clear fields of view of the perimeter barrier.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Defensive structures at the protected area boundary will be bullet-resistant and locked.

The protected area barrier and adjacent isolation zones will be patrolled by a guard or watchman at least once every two hours on a random path and with a random starting time.

## 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: Personnel access to the protected area must be through a locked door which is controlled by an individual protected by a structure which is bullet-resistant. (High Powered Rifle Rating)

Source: 73.55(d)(1)

Objective: Assure that protected area access is granted only by positive action by an individual. Assure that this individual has sufficient time to sound an alarm in the event of an attempt to gain protected area access by forceful means.

Review Procedures:

Security Plan Review:

Confirm that personnel access to the protected area is through a locked door.

Confirm that control of the locked door is by an individual protected by a bullet-resistant structure.

Questions and Comments:



Site Visit:

Additional Review:

Evaluation Findings:

Personnel access to the protected area will always be through a locked door which is controlled by an individual in a bullet-resistant structure.

#### 3.2.1.2 Physical Structures

There are no additional criteria.

#### 3.2.1.3 Locks, Keys, Combinations and Related Equipment

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

#### 3.2.1.4 Security Posts

Acceptance Criterion 3.2.1.4.A: Each portal must be operated by at least two members of the physical security force when open for normal personnel access.

Source: 73.55(d)(1), (2), (3)

Objective: Assure that adequate manpower is available to satisfactorily meet the requirements for search and access control.

Acceptance Criterion 3.2.1.4.B: Unauthorized entries through a personnel access portal shall be detected and communicated to the central and secondary alarm stations with a level of assurance consistent with Acceptance Criterion 3.1.4.A.

Source: 73.55(c)(4) [Staff interpretation of the level of detection capability required in order to assure that an adequate response can be made].

Objective: Assure that a consistent, high assurance level of detection is maintained against all types of unauthorized personnel penetrations of the protected area barrier.

Review Procedures:

Security Plan Review:

- A) Confirm the commitment to control personnel access by stationing two members of the physical security force at open portals: one in a bullet-resistant structure to control access, and the other to monitor and conduct searches.
- B) Confirm the commitment to alarm the doors giving access to the protected area.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

All portals will be operated by two members of the physical security force when open for personnel access.

Unauthorized entries through a personnel access portal will be detected and communicated to the central and secondary alarm stations with high assurance. When the portal is not open for access the door giving access to the protected area is locked and alarmed.

### 3.2.1.5 Search and Admittance Control Hardware

Acceptance Criterion 3.2.1.5.A: All search and admittance control hardware shall clearly annunciate warnings at the portal.

Source: 73.55(d)(1)

Objective: Assure that detections of violations by search and admittance control hardware are obvious to attending personnel so that appropriate action may be taken immediately. Assure that these detections cannot be ignored by an insider.

Acceptance Criterion 3.2.1.5.B: Prior to protected area entry all hand-carried or delivered packages shall be searched for devices such as firearms, explosives or incendiary devices, or other items which could be used for industrial sabotage.

Source: 73.55(d)(2), 73.55(b)(3)

Objective: Provide high assurance detection of unauthorized materials before protected area entry.

Acceptance Criterion 3.2.1.5.C: A search of all personnel entering the protected area shall be conducted to detect firearms, explosives and incendiary devices (see Appendix B).

Source: 73.55(d)(1)

Objective: Assure detection of firearms, explosives and incendiary devices carried by personnel prior to their entering the protected area.

Acceptance Criterion 3.2.1.5.D: At the point of protected area access all personnel must be identified and their authorization checked.

Source: 73.55(d)(1), 73.55(b)(3)

Objective: Assure that those granted protected area access meet the criteria for entry with or without escort, as appropriate.

Review Procedures:

Security Plan Review:

- A) Confirm a commitment to alarm all search and admittance control hardware.
- B) Confirm that all hand-carried or delivered packages will be searched for firearms, explosives, incendiary devices or other items used for industrial sabotage.

- C) Confirm the existence of statements requiring the search of all personnel prior to entry into the protected area. Search can be performed by either equipment or by physical means and is for the purpose of preventing firearms, explosives and incendiary devices from being brought into the protected area.
- D) Confirm that an individual's identity and authorization will be checked prior to admittance into the protected area.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Metal and explosive detectors will clearly annunciate warnings at the portal.

All hand-carried and delivered packages will be searched physically or with the following equipment: \_\_\_\_\_.

All personnel entering the protected area will be searched.

The identification/authorization of those previously issued picture badges which permit unescorted access will be accomplished by \_\_\_\_\_; for those seeking unescorted access without prior badging the following steps will be taken: \_\_\_\_\_. All those seeking escorted access will be checked for identification/authorization as follows: \_\_\_\_\_.

### 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 area without escort. These badges should show the access authorization level of an individual while in a protected or vital area and should be relinquished before leaving the protected 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 (1) nonemployee no escort required, (2) areas to which access is authorized, and (3) 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. This badge should be worn on the upper front portion of the body so as to be clearly visible (except when operational or health physics reasons dictate otherwise).

Source: 73.55(d)(5), (6)

Objective: Assure that level of access and escort requirement for all persons in the protected area is clearly discernible at all times. Minimize likelihood of badge compromise resulting from lost badges.

Review Procedures:

Security Plan Review:

Confirm the commitment to a picture badge system for the control of personnel admitted access to the protected area.

Question and Comments:



Site Visit:

Additional Review:

Evaluation Findings:

A numbered picture badge will be issued to all individuals granted unescorted access to the protected area. These badges will include the following features: \_\_\_\_\_. Those granted escorted access will be issued badges with the following features: \_\_\_\_\_. Badges will be displayed while inside the protected area perimeter.

### 3.2.1.7 Communications

Acceptance Criterion 3.2.1.7.A: The capability of continuous communication from each portal with the central and secondary alarm station must be provided.

Source: 73.55(f)(g) [Staff recommendation based upon need to assure timely communication of an alarm to permit adequate response by the security force].

Objective: Assure that detections can be rapidly transmitted to the central and secondary alarm stations.

Review Procedures:

Security Plan Review:

Confirm that the continuous communication requirement is met by two-way radios carried by the guards. Alternatively, hard-wired intercom meeting security requirements (normal plant PA system is not acceptable) may be used to meet this criterion.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

All personnel access portals are capable of continuous communication with the central and secondary alarm station.

### 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.

Source: 73.44(d)(4), 73.55(b)(3)

Objective: Provide a substantial measure of protection against the introduction of sabotage materials by vehicles.

Review Procedures:

Security Plan Review:

Confirm a commitment by the licensee to search all vehicles prior to entering the protected area. This includes company-owned vehicles which have left the protected area.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

All vehicles, except in emergency situations, will be thoroughly searched for sabotage materials including inspection of the cab, engine compartment, undercarriage and cargo area, prior to entering the protected area.

### 3.2.2.1 Layout

Acceptance Criterion 3.2.2.1.A: Vehicle access to the protected area will be controlled by an individual protected by a structure which is bullet-resistant.

Source: 73.55(d)(1)

Objective: Assure that detection of forceful protected area entry will be communicated to the central and secondary alarm stations.

Review Procedures:

Security Plan Review:

Confirm 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-resistant structure.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The opening of vehicle gates will be key-controlled, electronically-controlled. Control of the key, electronic door opener will rest with a member of the physical security force located in a bullet-resistant structure.

### **3.2.2.2 Physical Structures**

All vehicle portals which are part of the protected area perimeter barrier shall satisfy Acceptance Criterion 3.1.2.A.

### **3.2.2.3 Locks, Keys, Combinations and Related Equipment**

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



#### 3.2.2.4 Security Posts

Acceptance Criterion 3.2.2.4.A: All portals shall be operated by at least two members of the physical security force when vehicles are permitted access.

Source: 73.55(d)(1)

Objective: Assure that any forceful entry of the protected area is detected and communicated to the central and secondary alarm stations with high assurance.

Review Procedures:

Security Plan Review:

Confirm the commitment to control vehicle access by maintaining two members of the physical security force at the portal during time of vehicle access.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

All portals will be operated by at least two members of the physical security force when vehicle access procedures are being conducted. The individual controlling access will be protected by a bullet-resistant structure.

3.2.2.5 Vehicle and Cargo Search Hardware

There are no specific acceptance criteria.

### 3.2.2.6 Communications

Acceptance Criterion 3.2.2.6.A: The capability of continuous communication from each portal with the central and secondary alarm station must be provided.

Source: 73.55(d)(4) [Staff recommendation based upon need to assure timely communication of an alarm to permit adequate response by the security force].

Objective: Assure that detections can be rapidly transmitted to the central and secondary alarm stations.

Review Procedures:

Security Plan Review:

Confirm the commitment for a dedicated communication link between each portal and the primary and secondary alarm stations.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

All portals have the capability of continuous communication with the central and secondary alarm station.



## CHAPTER 4 - PROTECTED AREAS

### 4.1 LAYOUT

Acceptance Criterion 4.1.A: External loading and storage areas shall not, to the extent practicable, be within 20 feet of vital areas.

Source: 73.55(d)(4)

Objective: Prevent, to the extent possible, the approach of vehicles to the proximity of vital areas and eliminate the protection that could be afforded an adversary by stored material.

Acceptance Criterion 4.1.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. Sufficient separation (at least 20 feet) should be maintained to prevent bridging from barrier to barrier, thereby avoiding detection by the perimeter intrusion detection system.

Source: 73.55(c)(2)

Objective: Prevent the bridging of barriers and to permit accurate assessment of detections made at the perimeter.

Review Procedures:

Security Plan Review:

- A) Examine the drawings to confirm that external loading and storage areas are not adjacent to vital areas.
- B) Examine the drawings to confirm a commitment by the licensee to separate vital and protected area boundaries. A minimum distance of 20 feet is required as an isolation zone.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The licensee has designated a material receiving area which is not adjacent to any vital area. Except for unforeseen situations which may develop during a refueling or major maintenance outage, external storage and loading areas will not be within 20 feet of vital areas.

All protected area barriers will be separate from vital area barriers, except at \_\_\_\_\_.



#### 4.2 PHYSICAL STRUCTURES

There are no specific acceptance criteria for nonvital buildings, barriers and structures that stand in the protected area, except those used as security posts.

### 4.3 ILLUMINATION AND SURVEILLANCE

Acceptance Criterion 4.3.A: Illumination shall be maintained throughout the protected area including the top and sides of all accessible structures. A structure shall be judged accessible if it is less than 18 feet in height or ready means is provided for access to the roof, such as ladders or climbing bars. The minimum level of illumination shall be 0.2 footcandle measured horizontally at ground level.

Source: 73.55(c)(5) [Staff interpretation of the requirement for lighting buildings based upon military guidelines].

Objective: Assure that there are no dark areas or shadows in the protected area which could hide a crouching man from detection by the naked eye.

Acceptance Criterion 4.3.B: If systems are provided for surveillance of the protected area, capability shall be provided for transmission of equivalent surveillance data to the central and secondary alarm stations.

Source: 73.55(a) [Staff requirement based upon need to prevent false assessment by insider in central or secondary alarm station].

Objective: Assure accurate assessment cannot be subverted by an insider.

Review Procedures:

Security Plan Review:

- A) Confirm a commitment by the licensee to provide 0.2 footcandle of illumination throughout the protected areas.
- B) Confirm that a commitment to use surveillance systems to survey that portion of the protected area outside the isolation zone includes the display of the surveillance data in both the central and secondary alarm stations.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Illumination will be provided by a \_\_\_\_\_ lighting system. All exterior areas in the protected area will be illuminated to a minimum level of 0.2 footcandle including the top and sides of all buildings except \_\_\_\_\_, which exceeds 18 feet in height and permits no easy access to the roof.

A CCTV system will be employed to provide surveillance of the following sections in the protected area outside the isolation zone: \_\_\_\_\_  
\_\_\_\_\_. Equivalent surveillance data may be received by the central and secondary alarm stations using the following procedures:  
\_\_\_\_\_.

#### 4.4 SECURITY POST (FIXED AND MOBILE)

Acceptance Criterion 4.4.A: All physical structures in the protected area credited as defensive positions for response forces shall provide:

- 1) Bullet-resistance (High Power Rifle Rating).
- 2) Full fields of view and fire in assigned response area.
- 3) Audible and visible indication of intrusion alarms in assigned response area.

Source: 73.55(a) [Staff requirement based to define attributes of defensive positions referenced to in the statement of considerations].

Objective: Assure that responders in defensive positions are protected and capable of observing and bringing effective fire to bear in their area of responsibility.

Acceptance Criterion 4.4.B: All exterior areas within the protected area shall be patrolled at random intervals and on a random path to provide human, on-the-scene visual observation. Each part of the protected area shall be observed at least once every two hours. Patrolling personnel shall be capable of continuous communication with the central and secondary alarm stations. Procedures should be established for frequent status reporting to the central alarm station.

Source: 73.55(c)(4) [Frequency is staff requirement based upon need to control insider activity as well as covert attempts at protected areas; include in the descriptions the following]:

Objective: Assure the protected area receives close visual observation at unpredictable times to detect abnormal occurrences.

Review Procedures:

Security Plan Review:

- A) Confirm that any commitment to use defensive positions in the protected area; include in the descriptions the following:
  - 1) Bullet-resistance.
  - 2) Fields of view and fields of fire.
  - 3) Audible and visual intrusion alarms for the area of responsibility assigned to the defensive position.
- B) Confirm there is a commitment for security patrols of the protected area at least once every two hours, and patrol personnel report to the central alarm station.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

There will be \_\_\_\_\_ defensive positions in the protected area. These will be located \_\_\_\_\_. They will be bullet-resistant, locked when occupied, have full field of view and fire in assigned response area. Intrusion alarms in the assigned response area will be indicated visibly by a \_\_\_\_\_ and audibly by a \_\_\_\_\_.

All exterior areas within the protected area will be patrolled by a radio-equipped guard or watchman at least once every two hours.

#### 4.5 ESCORTS

Acceptance Criterion 4.5.A: All vehicles not licensee-designated shall be escorted in the protected area by a guard or other armed individual.

All visiting personnel shall be escorted by an individual who is authorized for unescorted access to the protected area and designated for escort duty. The ratio of escorts required for a visiting party shall depend upon the ability of the escort to monitor the activities of the group.

Source: 73.55(d)(4) !Staff requirement for armed escort based upon recognition of a vehicle as a potentially effective aid in sabotage with resulting need for strict control.

Objective: Assure strict control of nonlicensee-designated vehicles in the protected area when they present the potential for significant assistance in sabotage activities.

Assure that the actions of all protected area visitors are monitored so that any unauthorized activities will be detected.

##### Review Procedures:

##### Security Plan Review:

Confirm a commitment to provide armed guard escorts for all nonlicensee-designated vehicles. (See Review Guideline)

Confirm a commitment to provide escorts to personnel authorized access. Escorts are to be individuals authorized unescorted access to the protected area and have been designated for escort duty. The nominal escort ratio in the protected area is 10 to 1. A larger ratio shall be authorized by the plant superintendent or other authorized persons.

##### Question and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

All nonlicensee-designated vehicles will be escorted by armed guards.

All visiting personnel will be escorted by an individual authorized for escorted access and escort duty. The ratio of escorts to visitors will be assigned according to the following guidelines: \_\_\_\_\_





## CHAPTER 5 - VITAL AREA BOUNDARIES

Acceptance Criterion 5.A: 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 of sufficient strength to provide high assurance of protection against sabotage. More than one vital area may be located within a single protected area.

Source: 73.55(c)(1)

Objective: Assurance that vital equipment is protected by at least two barriers.

Acceptance Criterion 5.B: 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 nonwork-related activities shall not be authorized except for good cause shown by the licensee.

Source: 73.55(d)(4) [Staff interpretation of requirements for positive access control].

Objective: Assure that vital area access is limited to those with authorized need.

Review Procedures:

Security Plan Review:

- A) Confirm a commitment to locate all vital equipment in a vital area.

Confirm that all vital equipment has been included in the licensee's (applicant's) list of vital equipment.

Review vital areas to assure that they are contained within two physical barriers.

- B) Confirm a commitment for positive access control to the vital area includes:

- 1) Limiting access to authorized personnel.
- 2) Requiring positive identification prior to entry.
- 3) Requiring an established need for access.

4) Maintaining records of entry, exit and reason for entry.

5) A system for control within the vital area.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Access to all equipment designated as vital requires passage through at least two physical barriers.

A satisfactory program for personnel positive access control has been established. The need for access is established as follows: \_\_\_\_\_  
\_\_\_\_\_ Identification of the individual seeking access  
is accomplished by \_\_\_\_\_.

## 5.1 LAYOUT

There are no specific requirements for vital area layout.

## 5.2 PHYSICAL BARRIERS

### 5.2.1 Barrier Descriptions

Acceptance Criterion 5.2.1.A: All vital area barriers shall be resistant to penetration by explosive 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 or other openings in the barrier.

Source: 73.55(a) [Staff requirement based upon recognition that adversaries at the vital area must be delayed long enough to provide time for the response force].

Objective: To prevent entry or delay to allow time for the response force to confront and neutralize the intruder.

Acceptance Criterion 5.2.1.B: All emergency exits in vital area barriers must be locked and alarmed.

Source: 73.55(d)(7), 73.55(e)(3)

Objective: Assure that the opening of emergency exits are controlled and, if open for any reason, are detected.

Acceptance Criterion 5.2.1.C: Locks, keys, combinations and other related equipment should satisfy Acceptance Criterion 3.1.2.C.

Source: See 3.1.2.C

Objective: See 3.1.2.C

Review Procedures:

Security Plan Review:

- A) Confirm that the description of vital area barriers includes materials, thicknesses and the licensee's (applicant's) estimates of their penetration time. Penetration time estimates must be justified and should be consistent with experimentally determined barrier penetration time, such as the NBS tests. The penetration times are to be evaluated against response times in Chapter 14.
- B) Confirm the licensee's commitment to lock and alarm all vital area exit points.
- C) Confirm the licensee's commitment to adhere to Acceptance Criterion 3.1.2.C with respect to vital area barriers.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Each of the vital area barriers ( ) are constructed of the following penetration resistant materials: , respectively. All doors, windows and other openings in the barriers provide protection equal to that of the remainder of the structure. The penetration time for all vital area barriers is sufficiently long to allow the response force to arrive at the barrier before penetration is completed.

All emergency exits from the vital area are locked and alarmed.

### 5.2.2 Intrusion Detection Hardware

Acceptance Criterion 5.2.2.A: High assurance detection shall be provided for all vital area entries. Active (operating) alarm systems must be used to protect portals to vital areas. Alarm systems must satisfy the requirements of the "Interim Federal Specification: Alarm System, Interior, Security, Components For," W-A-00450-B (GSA-FSS).

Source: 73.55(d)(7), 73.55(e)(3)

Objective: To provide high assurance protection by detecting attempted penetration at the vital area barriers and access portals.

Acceptance Criterion 5.2.2.B: All alarm systems must be provided with standby electrical power, according to requirements of the "Interim Federal Specification," W-A-00450-B (GSA-FSS).

Source: 73.55(e)(2)

Objective: Assure that intrusion alarm systems continue to function normally in the event of loss of offsite power.

Acceptance Criterion 5.2.2.C: All intrusion alarm systems shall have a frequency of false and nuisance alarms such that the response capability is not degraded. The intrusion alarms should satisfy the frequency of false and nuisance alarms specified in Regulatory Guide 5.44 and Interim Federal Specification W-A-00450-B (GSA-FSS).

Source: 73.55(a) [Staff interpretation of requirement to achieve high assurance detection].

Objective: Assure that the frequency of false and nuisance alarms does not degrade the response capability.

Acceptance Criterion 5.2.2.D: All intrusion detection systems shall 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. These systems shall satisfy the tamper-indicating and self-checking requirements of Regulatory Guide 5.44 and Interim Federal Specification W-A-00450-B.

Source: 73.55(e)(2)

Objective: Assure that the effectiveness of the intrusion detection system cannot be intentionally degraded or remain degraded for more than one minute without compensation if the cause is system failure.

Acceptance Criterion 5.2.2.E: All intrusion detection system hardware must annunciate at the central and secondary alarm stations. The annunciation of an alarm shall indicate the type of alarm (e.g., intrusion alarm, emergency exit alarm, etc.) and location.

Source: 73.55(e)(1), 73.55(e)(2)

Objective: Assure that an insider cannot prevent response by ignoring an alarm and that the response can be made appropriate to the type of alarm received.

Acceptance Criterion 5.2.2.F: Compensatory measures shall be established and employed to assure an equivalent level of protection in the event of detection hardware outage.

Source: 73.55(g)(1)

Objective: Assure that intrusion detection performance is not degraded by a failure of detection hardware.

Review Procedures:

Security Plan Review:

- A) Confirm the licensee's (applicant's) commitment to providing high assurance detection to attempts to gain unauthorized access into vital areas through portals or any part of the barrier. When alarm systems are used they shall meet the minimum level identified in the Interim Federal Specifications.
- B) Confirm that the intrusion detection system conforms to Interim Federal Specification W-A-00450-B (GSA-FSS) and includes the following emergency power capability:
  - 1) An automatic switch over from primary power to emergency battery and generator or emergency battery power without causing an alarm, but there is an indication.
  - 2) Twenty-four hour operation without recharging batteries or refueling generators, unless fuel is onsite.
- C) Confirm that the intrusion detection system performance includes the following average false alarm and nuisance alarm specifications:
  - 1) False alarm rate not to be greater than one per week per zone.
  - 2) Nuisance alarm rate not to be greater than one per week per zone.



- 3) False alarm and nuisance alarm rate not to be greater than one per day per zone under continuous visual observation.
- D) Confirm that intrusion detection system description includes the following tamper-indicating/self-checking capability:
- 1) All enclosures are equipped with tamper switches or trigger mechanisms compatible with alarm switches.
  - 2) Trigger mechanism/tamper switches remain in operation when system is in ACCESS mode.
  - 3) Controls that affect sensitivity of alarm system are located within tamper-resistant enclosure.
  - 4) Signal lines connecting alarm relays with alarm monitors are supervised.
  - 5) Signal line connecting sensor electronics with processing electronics are supervised.
- E) Confirm that the intrusion detection system description includes the following alarm capability:
- 1) Annunciated in both the central and secondary alarm stations.
  - 2) Annunciates detection of an intruder.
  - 3) Annunciates failures of emergency power to properly operate the system in the event of primary power loss.
  - 4) Annunciates indication of tampering.
  - 5) Annunciates failure of aging components which cause system failure.
  - 6) The type of alarm annunciation shall indicate the type of problem (detection, power failure, tampering, system failure).
- F) Confirm that procedures are documented, which include the positioning of guards/watchmen, to provide visual coverage in or at the vital area, when there is a hardware outage.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

An intrusion alarm system is, will be installed which will detect individuals attempting unauthorized access to the vital areas. The alarm systems will comply, complies with "Interim Federal Specification: Alarm Systems, Interior, Security, Components For," W-A-00450-B (GSA-FSS).

The intrusion alarm system at the protected area perimeter will be provided with an onsite source of emergency power. This power system meets the requirements of Interim Federal Specification W-A-00450-B in that: switch over is automatic, there is indication of switch over but no alarm, and it is capable of sustaining operation for a minimum of 24 hours.

The intrusion alarm system will be installed to provide, on the average, no more than one false and one nuisance alarm per zone per day, thus meeting the requirements of Regulatory Guide 5.44 and Interim Federal Specification W-A-00450-B (GSA-FSS).

The intrusion alarm system will satisfy the tamper-indicating and self-checking requirements of Regulatory Guide 5.44 and Interim Federal Specification W-A-00450-B. All equipment enclosures and sensitivity controls will be equipped with tamper switches or triggering mechanisms which operate even when the system is in the ACCESS mode. All signal lines connecting alarm relays with alarm monitors are supervised. The system will be self-checking. All intrusion detection system hardware will annunciate at both the central and secondary alarm stations and will indicate the type and location of the alarm.

Compensatory measures have been established and will be employed to provide an equivalent level of protection in the event of intrusion detection hardware outage. In the event of failure in a single area, a single guard or watchman will be posted to continuously observe the affected area.

D

### 5.2.3 Control Room

Acceptance Criterion 5.2.3: The walls, doors, ceiling, floor and any windows in the walls and doors of the control room shall be bullet-resistant. (High Power Rifle Rating)

Source: 73.55(e)(1)

Objective: To provide the level of protection required by regulation and to be consistent with the level of protection provided by most critical facilities.

Review Procedures:

Security Plan Review:

Confirm that a description of the control room includes specification for bullet-resistant walls, doors, ceiling, floor, windows and doors.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The walls, doors, ceiling, floor and any windows in the control room are bullet-resistant.

### 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 through a vital area boundary whether or not he is located (other than during temporary compensatory measures) 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.

Source: 73.55(d)(7)

Objective: Assure that vital area access is granted only by positive action by an individual. Assure that this individual has sufficient time to sound an alarm in the event of an attempt to gain vital area access by forceful means.

Review Procedures:

Security Plan Review:

Confirm that personnel access to vital area is through locked doors.

Confirm that control of the locked door is by an individual protected by a bullet-resistant structure.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Personnel access to all vital areas will always be through a locked door which is controlled by an individual in a bullet-resistant structure.

#### 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 in addition 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.

Source: 73.55(d)(7)

Objective: Assure that detections of violations by access control hardware are obvious to attending personnel so that appropriate action may be taken immediately. Assure these detections cannot be ignored by an insider.

Review Procedures:

Security Plan Review:

Confirm a commitment to alarm all access control hardware such as key card readers.

.. Confirm that activated alarms will be annunciated in both the central and secondary alarm stations.

Questions and Comments:



Site Visit:

Additional Review:

Evaluation Findings:

Key card readers will signal alarms in the central and secondary alarm stations when an invalid card is read. The alarms clearly indicate the attempted valid entry attempt by \_\_\_\_\_.

#### 5.3.1.6 Badge Control System

Acceptance Criterion 5.3.1.6.A: The numbered picture badge identification system used for all individuals, who are authorized access to the protected areas without escort, shall indicate the vital areas to which access is authorized, and should be relinquished before leaving the protected area. An individual not employed by the licensee but who requires frequent and extended access to vital areas may be authorized unescorted access to such areas provided his picture badge indicates the vital areas to which he is authorized access and which must be returned upon exit from the protected area and which indicates (1) nonemployee no escort required; (2) areas to which access is authorized; and (3) the period for which access is authorized. Individuals not authorized by the licensee to enter vital areas without escort shall be badged to indicate that an escort is required and the vital areas authorized. Badges shall be displayed at all times. This badge should be worn on the upper front portion of the body to be clearly visible (except for operational or health physics reasons).

Source: 73.55(d)(7)

Objective: Assure level of access and escort requirement for all persons in the vital area is clearly discernible at all times. Minimize likelihood of badge compromise resulting from lost badges.

Review Procedures:

Security Plan Review:

Confirm the commitment to a picture badge system which includes the control of personnel permitted access to vital areas.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The numbered picture badge issued to all individuals granted protected area access is coded in the following manner to indicate the vital areas granted access: \_\_\_\_\_ . Badges will be displayed while inside the protected area perimeter.

#### 5.3.1.7 Communications

Acceptance Criterion 5.3.1.7.A: Continuous communication capability must be provided from each portal at a vital area boundary with the central and secondary alarm station.

Source: 73.55(f)(1) !Staff recommendation based upon need to assure timely communication of an alarm to permit adequate response by the security force1.

Objective: Assure that detections can be rapidly transmitted to the central and secondary alarm stations.

Review Procedures:

Security Plan Review:

Confirm the commitment for a dedicated communication link between each vital area boundary post and the central and secondary alarm stations.

This requirement can be met by the security force two-way radio.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Each post at a vital area boundary portal has continuous communications capability with the central and secondary alarm station.

### 5.3.2 Vehicle Access Portals and Posts

#### 5.3.2.1 Physical Structures

There are no requirements in addition 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. This is in addition to the armed escort which must remain with the vehicle.

Source: 73.55(d)(7)

Objective: Assure that any unauthorized entry into a vital area is immediately detected and communicated to the central and secondary alarm stations.

Review Procedures:

Security Plan Review:

Confirm the commitment to control vehicle access to the vital area by posting a guard at the access portal during vehicle ingress and egress.

Confirm that the guard controlling vehicle access is in addition to the guard escorting the vehicle.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

At least one guard is posted at all vital area vehicle portals during vehicle ingress and egress. This guard is in addition to the guard performing vehicle escort duties.



### 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.

Source: 73.55(f)(1) [Staff recommendation based upon need to assure timely communication of an alarm to permit response by the security force].

Objective: Assure that detections can be rapidly transmitted to the central and secondary alarm stations.

Review Procedures:

Security Plan Review:

Confirm the commitment for a dedicated communication link between each vital area vehicle access security posts and the central and secondary alarm stations. This criterion may be met with the guard's two-way radios.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Each fixed post at a vehicle access portal is capable of continuous communications with the central and secondary alarm station.

## 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.

Source: 73.55(e)(1), 73.2(h)

Objective: To assure that the security provided for the control of security forces is consistent with that of facilities which they are protecting.

Review Procedures:

Security Plan Review:

Confirm the commitment to consider the onsite central alarm station a vital area.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The licensee has established a central alarm station which meets the criteria of a vital area as defined by 73.2(h).

### 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.

Source: 73.55(e)(1)

Objective: To provide assurance that an intruder cannot easily locate the central alarm station or affect the operation of the central alarm station from outside the protected area perimeter. Also, to assure there are no activities performed inside the central alarm station which could detract from the alarm response function.

Review Procedure:

Security Plan Review:

Confirm the commitment to locate the central alarm station in a building such that its interior is not visible from the perimeter of the protected area.

Confirm that the central alarm station does not contain any operational activities that would interfere with the execution of the alarm response function.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The central alarm station is located in the interior of building           . The interior of the central alarm station is not visible from the perimeter of the protected area.

## 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-resistant. (UL 752, High Power Rifle Rating)

Source: 73.55(e)(1)

Objective: To provide the level of protection required by regulation and to be consistent with the level of protection provided the facilities.

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 six inches) must be kept locked at all times.

Source: 73.55(a) [Staff requirement based on need to provide high assurance that an insider or intruder cannot gain control of the response force or vital/protected area portals through use of the central alarm station].

Objective: To provide high assurance that the central alarm station functions cannot be compromised without overt action from outside the alarm station to gain admittance.

Review Procedures:

Security Plan Review:

Confirm that a description of the central alarm station includes specification for bullet-resistant walls, ceiling, floor, windows and doors.

Confirm the commitment to keep all central alarm station portals, as described above, locked at all times.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The central alarm station is constructed such that the walls, ceiling, floor, doors and windows are bullet-resistant. (UL 752, High Power Rifle Rating)

All portals which would permit personnel entry are kept locked at all times.



### 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.

Source: 73.55(e)(1)

Objective: To provide rapid warning of security violations.

Acceptance Criterion 6.1.3.B: The annuciation 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 the knowledge of secondary alarm station operator.

Source: 73.55(e)(2)

Objective: To provide information to the central alarm station for situation assessment and rapid response. Also to reduce the likelihood of an insider controlling alarms from the central alarm station.

Acceptance Criterion 6.1.3.C: The central alarm station must be capable of performing all required operations on emergency power.

Source: 73.55(e)(1), 73.55(e)(2) [Staff requirement based upon the need to assure protection is not degraded when there is a power failure].

Objective: To assure the capability to provide rapid response is not degraded because of the loss of the primary power system.

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, 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.

Source: 73.55(e)(2)

Objective: Assure that the effectiveness of the central alarm station systems cannot be degraded or remain degraded.

Review Procedures:

Security Plan Review:

- A) Confirm the commitment of the licensee to have all alarms annunciate in the CAS within one second of alarm activation.
- B) Confirm the commitment to assure that the central alarm station alarm annunciation will indicate the type of alarm and its location.  
Confirm a commitment to assure that the central alarm station operator cannot change an alarm point status or actuate any locking or controlling device at protected or vital area portals without the knowledge of the secondary alarm station operator.
- C) Confirm the commitment to provide emergency power to the central alarm station.
- D) Confirm that central alarm station systems description includes tamper-indicating/self-checking capability.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The alarms in the central alarm station will annunciate within one second of alarm activation. Annunciators meet the requirements of Interim Federal Specification W-A-00450-8 with respect to unit compatibility, access/secure and reset switches, readout, construction and connections.

Alarm annunciation is provided in the central alarm station for the following types of alarms: \_\_\_\_\_. The location of alarm activation is also provided. The alarm system is designed to prevent the central alarm station operator from changing any alarm point status or actuating any locking or controlling device at protected or vital area portals without the knowledge of the secondary alarm station operator.

The annunciator and other alarm or surveillance system hardware, including transmission lines, are tamper-indicating and self-checking.

The central alarm station will be provided with an onsite source of emergency power. This power system provides automatic switch over with an indication of switch over but no alarm.

#### 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.

Source: 73.55(e)(1)

Objective: To provide for rapid response to alarms, assessment of alarms, alerting of security force and the initiation of countermeasures to resolve the situation.

Review Procedures:

Security Plan Review:

Confirm the commitment to have at least one member of the security organization in the central alarm station at all times.

Confirm that the duties of at least one member of the security force located in the central alarm station are totally dedicated to security monitoring.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The central alarm station is continuously manned by a member of the security organization at all times. This member is totally dedicated to duties of security monitoring.

#### 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.

Source: 73.55(F)(1), (2), (3)

Objective: To provide assurance that there will always be communication links to local law enforcement authorities, plant physical security force, and the plant control room.

Review Procedures:

Security Plan Review:

Confirm the commitment to provide the following communication capability with the central alarm station.

Wire (e.g., telephone) and wireless (e.g., radio or microwave) plant control room with them (unless they are colocated).

Wire (e.g., telephone) and wireless (e.g., radio or microwave) communication with the local law enforcement authorities.

Wireless communication with members of the physical security force on patrol.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Redundant and independent communication from the central alarm station to (LLEA) is provided by \_\_\_\_\_ and \_\_\_\_\_ system. Communication to the plant control room is provided by \_\_\_\_\_ and additional communication to fixed post is provided by \_\_\_\_\_. Wireless communications with members of the physical security force on patrol is provided by \_\_\_\_\_.

## 6.2 SECONDARY ALARM STATIONS

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.

Objective: To assure that a single act cannot remove the capability of receiving and responding to alarms.

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 the knowledge of the central alarm station operator.

Source: 73.55(e)(2)

Objective: To prevent, with high assurance, an insider working at the secondary alarm station from controlling alarms or locking and controlling devices at protected and vital area portals.

Acceptance Criterion 6.2.C: The secondary alarm station must satisfy the following requirements: (1) contains no operational function which would interfere with the execution of the alarm response function, (2) is locked at all times, (3) has annunciators and other surveillance hardware which are all tamper-indicating and self-checking, and (4) is capable of fully independent and redundant communications with local law enforcement, plant control room (if not colocated with the secondary alarm station) and continuous communication with physical security force.

Source: 73.55(e)(1), 73.55(e)(2), 73.55(a) [Staff requirement based on need to provide high assurance that an insider or intruder cannot gain control of the response force or vital or protected area portals through use of the secondary alarm station].

Objective: To provide a backup capability to the central alarm station.

Review Procedures:

Security Plan Review:

- A) Confirm the commitment of the licensee to have a secondary alarm station in addition to the central alarm station.

Confirm that the alarms annunciate within one second of sensor activation and that the annunciator hardware meets Interim Federal Specification W-A-00450-B.



If located onsite, the secondary alarm station should be protected as a vital area and, therefore, complies with Acceptance Criteria 6.1.1.A and 6.1.2.B.

Confirm that the secondary alarm station is continuously manned.

- B) Confirm a commitment to assure that the secondary alarm station operator cannot change an alarm point status or actuate and locking or controlling device at protected or vital area portals without the knowledge of the central alarm station operator.
- C) Confirm the commitment to provide the secondary alarm station, with capabilities that satisfy the requirements of Acceptance Criteria 6.1.3.D (Alarm and Surveillance Monitoring Hardware) and 6.1.5.A (Communications). Confirm that the secondary alarm station is locked at all times and that the operator is not assigned duties which will interfere with his alarm response function.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The secondary alarm station is continuously manned by \_\_\_\_\_ members of the security organization, is located onsite in building \_\_\_\_\_. Alarms will annunciate within one second of alarm activation and meet the requirements of Interim Federal Specification W-A-00450-B with respect to unit compatibility, access/secure and reset switches, readout, construction and connections.

The secondary alarm station operator is not 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 the knowledge of the central alarm station operator.

\_\_\_\_\_, \_\_\_\_\_ and \_\_\_\_\_ functions performed in the secondary alarm station will not interfere with the execution of the alarm response functions. The secondary alarm station systems will satisfy the tamper-indication and self-checking requirements of Regulatory Guide 5.44. All equipment enclosures and sensitivity controls will be equipped with tamper switches or triggering mechanisms which operate even when the system is in the ACCESS mode. All signal lines connecting alarm relays with alarm monitors are supervised. All access portals to the secondary alarm station are locked at all times. Redundant and independent communication from the secondary alarm station to (LLEA) is provided by \_\_\_\_\_ and \_\_\_\_\_ systems. Communications to the plant control room is provided by \_\_\_\_\_ and \_\_\_\_\_ systems. Communications to guards either at fixed post or on patrol is provided by \_\_\_\_\_ and additional communication to fixed post is provided by \_\_\_\_\_.

### 6.3 OTHER VITAL AREAS

Acceptance Criterion 6.3.A (Alternative 1): All access to the very limited number of vital locations, such as containment, wherein acts conducted entirely within this location could result in successful industrial sabotage, must include at least two personnel authorized for unescorted access to vital areas.

Source: 73.55(a) [Staff requirement based upon need to provide high assurance protection against the insider].

Objective: To reduce the likelihood of an employee performing acts of industrial sabotage or attempting such acts without immediately attracting someone's attention.

Acceptance Criterion 6.3.A (Alternative 2): Compartments are used to eliminate a single authorization providing access to a vital area wherein action taken entirely within that location could result in successful sabotage.

Source: 73.55(a) [Staff requirement based upon need to provide high assurance protection against the insider].

Objective: To reduce the likelihood of an employee performing acts of industrial sabotage or attempting such acts in locations where two or more controls must be effected.

Review Procedures:

Security Plan Review:

- A) Confirm the commitment by the licensee to identify all "type 1" vital locations.
- B) Confirm the commitment to have adequate "two-man" rule in effect in "type 1" vital area locations. The "two-man" rule requires at least two men with equivalent knowledge in the "type 1" location or a surveillance monitoring system which can provide the same level of protection.

Confirm the commitment by the licensee (applicant) to place vital equipment in secure compartments which require positive control for entry.

The barrier should meet or exceed the strength of 11 AWG wire mesh secured at floor (and ceiling, if appropriate).

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_ and \_\_\_\_\_ identified "type 1" vital locations cannot be entered by a single employee. Lists of employees who are authorized entrance to "type 1" locations are maintained by security members controlling access. These security members are instructed that single employees are not to be permitted entry.

Vital controls and equipment are enclosed by \_\_\_\_\_. Access control is provided by \_\_\_\_\_ and \_\_\_\_\_ which provides positive action such that the possibility of a single authorization providing access is virtually eliminated.

### 6.3.1 Surveillance Hardware

Acceptance Criterion 6.3.1.A: If used, all surveillance system hardware must be self-checking and tamper-indicating.

Source: 73.55(e)(2)

Objective: To be immediately aware of system degradation or manipulation by an adversary so that compensatory measures can be taken to maintain high assurance protection.

Acceptance Criterion 6.3.1.B: If used, surveillance hardware must provide the same information to the central and secondary alarm stations.

Source: 73.55(e)(1)

Objective: Assure that an insider cannot prevent response by ignoring information and alarms and that rapid response can be made.

Review Procedures:

Security Plan Review:

- A) If used, confirm the commitment to assure that all hardware includes tamper-indicating/self-checking capability.
- B) Confirm that any surveillance hardware provides the same information in both the central and secondary alarm stations.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

All surveillance system hardware will be tamper-indicating and self-checking.

The \_\_\_\_\_ surveillance hardware provides the same information to both the central and secondary alarm stations. Hardware alarms will actuate in both the central and secondary alarm stations.

### 6.3.2 Security Posts (Fixed and Mobile)

Acceptance Criterion 6.3.2.A: Consistent with operating constraints, all vital areas should be visually inspected at least once each shift by a member of the plant staff.

Source: 73.55(a) [Staff requirement based on the need to assure that activities by an insider are not in progress].

Objective: To reduce the likelihood that an insider normally assigned to work in a vital area could sabotage the facility.

Acceptance Criterion 6.3.2.B: If used, all fixed security posts in the vital area should provide continuous communication capability with the central and secondary alarm stations.

Source: 73.55(f)(1) [Staff recommendation based upon need to assure timely communication of an alarm to permit response by the security force].

Objective: Assure that security personnel in vital areas can provide warning and receive direction during incident response.

Review Procedures:

Security Plan Review:

- A) The licensee should provide for a system of surveillance for internal vital areas. This should include a tour by a plant staff member of all vital areas (except those where it would be hazardous to health and safety) at least once each shift. During this tour a visual inspection should be made.
- B) Confirm the commitment for a dedicated communication link between any fixed security post located in a vital area and the central and secondary alarm stations.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

A tour of all vital areas except \_\_\_\_\_ will be conducted during each shift by \_\_\_\_\_ or \_\_\_\_\_.

In addition to radios carried by guards, all fixed security posts located in vital areas have \_\_\_\_\_ type dedicated communication to the central and secondary alarm station. This system provides a continuous communication capability with radio backup.



### 6.3.3 Escorts

Acceptance Criterion 6.3.3.A: All visiting personnel in the vital area shall be accompanied by an escort.

Source: 73.55(6), 73.55(7) [Staff requirement to maintain close surveillance over personnel not normally authorized access to vital areas].

Objective: Assure that the actions of all vital area visitors are monitored so that any unauthorized activities will be immediately detected.

Acceptance Criterion 6.3.3.B: Provide armed escorts for vehicles in the vital areas.

Source: 73.55(d)(4)

Objective: Assure strict control of nonlicensee vehicles in the vital areas when they present the potential for providing assistance to sabotage activities.

Review Procedures:

Security Plan Review:

- A) Confirm the commitment to provide escorts to visiting personnel authorized access to vital areas. Escorts are to be individuals authorized unescorted access to the vital area to be visited and have been designated for escort duty. The nominal escort ratio in vital areas is five to one. A larger ratio shall be authorized by the plant superintendent or other authorized persons.
- B) Confirm a commitment by the licensee to provide armed escorts when escorting vehicles inside the vital areas.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

All personnel visiting vital areas will be escorted by an individual authorized unescorted access and escort duty. The ratio of escorts to visitors has been set at \_\_\_\_\_ to \_\_\_\_\_ which satisfies the requirement.

All nonlicensee-designated vehicles will be escorted by armed guards.

## CHAPTER 7 - CENTRAL COMMUNICATIONS SYSTEMS

### 7.1 TELEPHONE SYSTEM

Acceptance Criterion 7.1.A: All telephone closets, unattended switchboards and any locations within the plant where the ability to telephone internally and/or externally could be significantly disrupted shall be locked.

Source: 73.55(a) [Staff requirement based upon the importance of communication for response force direction and control, coordination with other plant operations and for requesting offsite assistance from law enforcement agencies and others].

Objective: To provide with high assurance that a communication system will be available for direction, control and liaison with the facility's organization and offsite organizations.

Review Procedures:

Security Plan Review:

Confirm the commitment to safeguard the facility's telephone system by providing locks to telephone closets, unattended switchboards, and other locations where the telephone system could be significantly disrupted.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Telephone closets located at \_\_\_\_\_ are locked. The switchboard located \_\_\_\_\_ is locked from \_\_\_\_\_ to \_\_\_\_\_ and other periods when unattended.

## 7.2 INTERCOM AND PUBLIC ADDRESS SYSTEM

Acceptance Criterion 7.2.A: Where used as part of the security system protect with locks and alarms any locations within the plant where the ability to use the intercom or public address systems could be largely or totally disrupted.

Source: 73.55(a) [Staff requirement based upon the need to maintain communication for response force direction and control, and coordination with other facility activities].

Objective: To provide with high assurance that communications, with the security organization and other facility activities, cannot be easily disrupted.

Acceptance Criterion 7.2.B: All intercom and public address systems used as part of the security communication system should be provided with an onsite source of emergency power.

Source: 73.55(f)(4)

Objective: To assure, in the event of a power failure, communications will not be degraded.

### Security Plan Review:

- A). Confirm the commitment to protect critical locations of intercom (or public address) systems used as part of the security communication system. Protection should be provided by locks and alarms.
- B) If the intercom (or public address) is used as part of the security communication system, determine if a commitment is made for providing it with emergency power.

### Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The \_\_\_\_\_ public address system used by security during response to safeguard incidents has critical component locations at \_\_\_\_\_ and \_\_\_\_\_. These locations are locked and alarmed at all times to protect the system from becoming largely or totally disrupted.

\_\_\_\_\_ will provide emergency power to the intercom system during primary power failures. This emergency power system will provide for 24 hours of continuous use without battery recharging.

### 7.3 OTHER CENTRAL COMMUNICATIONS SYSTEMS

Acceptance Criterion 7.3.A: 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.

Source: 73.55(a) [Staff requirement based upon the need to provide a consistent level of protection to all communications used by security].

Objective: To maintain communication with response forces and facility activities during safeguards incidents.

Review Procedures:

Security Plan Review:

- Confirm the commitment to protect all central communication systems which are critical to directing and controlling response forces.

- Confirm the commitment to provide these systems with an emergency power system.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

The \_\_\_\_\_ and \_\_\_\_\_ communication components, systems are critical to the central communication system and are protected by \_\_\_\_\_ lock and \_\_\_\_\_ alarm system. Emergency power can be provided for up to 24 continuous hours of operation by \_\_\_\_\_.



## CHAPTER 8 - RESPONSE TO SECURITY CONTINGENCIES

### 8.1 RESPONSE FORCE AVAILABILITY

Acceptance Criterion 8.1: The operational duties of armed response individuals must not interfere with their ability to perform response tasks.

Source: 73.55(b)(4)

Objective: To have a force of reserve personnel available at the facility for immediate response to security alarms.

Review Procedures:

Security Plan Review:

Confirm the commitment to provide armed response individuals.

Confirm the commitment to assure that any routine or emergency duties assigned to armed response individuals will not interfere with their response tasks.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

There are \_\_\_\_\_ armed response individuals assigned each shift. They are assigned routine duties of \_\_\_\_\_ and \_\_\_\_\_ which do not interfere with their ability to perform their response tasks.

## 8.2 ASSIGNMENT OF RESPONSIBILITIES

Acceptance Criterion 8.2.A: Demonstrate that security procedures exist which will be used for responding to the contingencies given in Appendix A. The procedures must explain when and how the security organization will take action to execute these procedures.

Source: 73.55(h)(3)

Objective: To provide, with high assurance, that the security organization can respond effectively and efficiently to attempted threats and sabotage.

Review Procedures:

Security Plan Review:

Confirm the commitment to have documented security procedures which include (1) the contingency incidents for which the procedures are applicable (must include those from Appendix A), and (2) a discussion of when the plan is to be put into effect and what is to be accomplished (must cover the material given in Appendix A).

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Procedures for responding to the following contingencies are documented and located at \_\_\_\_\_. Contingencies: \_\_\_\_\_ The procedures include a discussion of objectives, decision and actions, required information and materials and an identification of the individual responsible for carrying out specific actions or making specific decisions. Also included are the procedures for: (1) threat identification and assessment, (2) requesting assistance from local law enforcement agencies, (3) guards and armed response force individuals to interpose themselves between vital areas and adversaries, and (4) to prevent delay or use deadly force against an adversary.

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

Acceptance Criterion 9.A: Develop and maintain provisions to assure that there will be no increase in the likelihood of successful industrial sabotage during refueling and major maintenance operations.

Source: 73.55(b)(3), 73.(d)(8)

Objective: To assure safeguards exist to reduce the plant's vulnerability to sabotage during maintenance and repair 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.

Source: 73.55(a) [Staff estimate based on the requirement to provide high assurance protection].

Objective: To prevent industrial sabotage resulting from adversary action under the cover of refueling/major maintenance operations.

Review Procedures:

Security Plan Review:

- A) Confirm a commitment by the licensee to give high assurance that the level of security during maintenance and refueling operations does not lessen and increase the likelihood of sabotage.
- B) Confirm the commitment to perform testing and inspection of any vital areas where maintenance has been performed during refueling/major maintenance operations.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Finding:

The security procedures include procedures to place into effect during refueling or \_\_\_\_\_, and \_\_\_\_\_ major operation.

Inspection and testing procedures consisting of \_\_\_\_\_ to be implemented following \_\_\_\_\_ provide high assurance protection against the likelihood of sabotage resulting from maintenance/refueling activities.

## CHAPTER 10 - 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.

Source: 73.55(a) [Staff requirement based upon the need to provide high assurance protection at all times].

Objective: To assure that security provided to the reactor facility is not diminished during periods when construction operations are underway at an adjacent site.

### Review Procedures:

Confirm the level of physical protection afforded a plant site is not diminished by construction operations at any adjacent site.

### Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

During periods of construction at adjacent sites the security organization will: \_\_\_\_\_. This provides a level of protection equivalent to that which exists when construction is not present.



## CHAPTER 11 - OVERALL PHYSICAL SECURITY PROGRAM PERFORMANCE

Acceptance Criterion 11.A: Demonstrate that the physical security system shall satisfy the general performance requirement, that is, provides high assurance protection against industrial sabotage.

Source: 73.55

Objective: To assure that the integrated components of the physical security system provide satisfactory protection.

Acceptance Criterion 11.B: Justify all parameters and their values used to simulate adversary delay, intrusion detection performance, surveillance systems performance, search and admittance control hardware performance and access control hardware performance. Also justify parameters and their values used to simulate the response force, supporting law enforcement.

Source: 73.55

Objective: To assure that the results obtained from the security system evaluation are based on valid information and can therefore be assumed to be valid.

Review Procedures:

Security Plan Review:

- A) Confirm that an evaluation of the plant's physical security system has been made. The evaluation may make use of computer models such as EASI, TSO, or use manual quantitative techniques. The evaluation should include an integrated examination of potential adversary paths, the time required for the adversary to travel through the facility, the number of guards (armed response individuals) available to intercept the adversary, and the time for guards (armed response individuals) to intercept the adversary. Other parameters to be considered as part of this evaluation are those which represent the performance of detectors, alarm systems and communication systems. Delay times associated with information evaluation and decision making should also be considered in the analyses.
- B) Confirm that all parameters and their values used to evaluate the physical security systems performance are justified. The following systems, if used in the evaluation, should have their performance parameters identified and values justified:

1. Adversary performance.
2. Detection performance.
3. Surveillance performance.
4. Search and admittance performance.
5. Access control performance.
6. Response force performance.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Integrated safeguards systems performance has been demonstrated using \_\_\_\_\_ model, technique. This technique considers adversary paths and times, response times and paths, decision delays and parameters representative of detection, alarm and communication systems, and barrier performance.

Parameters and their values used to evaluate the performance of the physical security system have been extracted from \_\_\_\_\_ accepted source documents. Justification is provided for changes to parameter or parameter values.



## 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.

Source: 73.55(g)(1)

Objective: To assure that barriers and their access points remain in workable order and function as intended.

Review Procedures:

Security Plan Review:

Confirm the commitment for an inspection, test and maintenance program.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Barrier and access portals inspection, test and maintenance procedures are established which includes all the protected area and vital area barriers and portals.

## 12.2 ALARMS, ANNUNCIATORS AND SURVEILLANCE SYSTEMS

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.

Source: 73.55(g)(2)

Objective: To assure that intrusion alarms are in working order and therefore can be depended upon.

Review Procedures:

Security Plan Review:

Confirm the commitment to establish an intrusion alarm inspection test and maintenance program.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

An intrusion alarm system inspection test and maintenance program is established. These tests will be conducted at the beginning and end of any period the system is used for security but at least once every seven days. All alarm systems, performance and calibration tests, and maintenance performed is documented.



### 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.

Source: 73.55(g)(1)

Objective: To assure that special purpose detectors are in working order and therefore can be depended upon.

Review Procedures:

Security Plan Review:

Confirm the commitment to establish a special purpose detector inspection, test and maintenance program.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

A special purpose detection system inspection test and maintenance program is established. These tests will be conducted at least once every seven days. All detector systems, performance and calibration tests and maintenance performed is documented.

#### 12.4 COMMUNICATIONS EQUIPMENT

Acceptance Criterion 12.4.A: 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.

Source: 73.55(g)(3)

Objective: To assure that all communication systems used for security are in working order and therefore can be depended upon.

Review Procedures:

Security Plan Reveiw:

Confirm the commitment to establish a communication inspection, test and maintenance program.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

A communication systems inspection test and maintenance program will be, is established. The program includes tests of all offsite communication equipment at least once every \_\_\_\_\_, and onsite communication equipment at least once at the beginning of every security shift.

## 12.5 SECURITY PERSONNEL EQUIPMENT

Acceptance Criterion 12.5.A: All security personnel equipment, including weapons, protective clothing and vehicles, shall be maintained in operational condition.

Source: 73.55(g)(1)

Objective: To assure that equipment used by security personnel is serviceable and in excellent working order.

Review Procedures:

Security Plan Review:

Confirm the commitment to establish a program to inspect, test and maintain security personnel equipment.

Question and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Equipment used by security personnel will be inspected and maintained in accordance with an established planned inspection and maintenance program.

## CHAPTER 13 - SECURITY RECORDS

Acceptance Criterion 13.A: All security records shall be maintained at the site and retained for the period indicated below, but in no case for less than one year:

- (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) Individual security training records shall be maintained for the period of employment in the security force.
- (4) Records of an individual's access to locks, keys, combinations and other related equipment shall be maintained for period of employment or for the duration that such locks, keys and combinations are in use.

Source: 73.55(b) [Staff requirement based upon good management practices for control, evaluation and development of the security organization].

Objective: To provide documentation usable to reconstruct past situations requiring investigations and to provide materials for control, evaluation and to further develop the physical security organization.

Review Procedures:

Security Plan Review:

Confirm the commitment to maintain security records onsite for a period of at least one year or for the period specified above.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

All security records are maintained onsite for a period of at least one year and the following security records are maintained for the period specified below:

- (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) Individual security training records shall be maintained for the period of employment in the security force.
- (4) Records of an individual's access to locks, keys, combinations and other related equipment shall be maintained for period of employment or for the duration that such locks, keys and combinations are in use.



### 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 and inspections performed on physical barriers, intrusion alarms, communications equipment and other security-related equipment.

Source: 73.70(e)

Objective: To provide referenceable records for use in evaluating systems performance with time.

Review Procedures:

Security Plan Review:

Confirm the commitment to documenting all routine security tours and inspections, tests and inspections, performed on physical barriers, intrusion alarms, communication equipment, and other security-related equipment.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Records of security tours and inspections, and test and inspections of  
                     are maintained.

## 13.2 MAINTENANCE

Acceptance Criterion 13.2.A: Establish and maintain a system for documenting all maintenance action performed on physical barriers, intrusion alarms, communication equipment and other security-related equipment.

Source: 73.70(e)

Objective: To provide referenceable records usable for evaluating systems performance, reliability and maintainability.

Review Procedures:

Security Plan Review:

Confirm the commitment to maintain records of maintenance performed on physical barriers, intrusion alarms, communication equipment, CCTV, emergency power supplies and other security-related equipment.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Records are maintained for all maintenance performed on physical barriers, intrusion alarms, communication equipment, CCTV, emergency power supplies and other security-related equipment.

### 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.

Source: 73.70(f)

Objective: To provide a measure of the validity of an alarm system.

Review Procedures:

Security Plan Review:

Confirm the commitment to recording the following data relative to alarm systems:

- A) Date and time of alarm annunciation.
- B) Type of alarm.
- C) Location of alarm detector.
- D) Alarm circuit.
- E) Determination of cause (intrusion, alarm check, false alarm, tamper, or failure).

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Records of each alarm annunciation are maintained by the \_\_\_\_\_  
and located at \_\_\_\_\_. Information recorded for an alarm  
annunciation includes date and time, type, location, circuit and cause.

#### 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.

Source: 73.70(f)

Objective: To provide a record usable for evaluation and improving response.

Review Procedures:

Security Plan Review:

Confirm the commitment to document the security organization's actions when responding to alarms, intrusions and other security incidents.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Security response records are maintained by \_\_\_\_\_ located at \_\_\_\_\_ . Information documented in these records includes date and time of incident, nature of incident, type and number of responders, response action and an assessment of response action.



### 13.5 AUTHORIZED INDIVIDUALS

Acceptance Criterion 13.5A: Establish and maintain a record of all persons who have been authorized access to protected areas.

Source: 73.70(a)

Objective: To maintain historical information useful for evaluation of potential security-related problems.

Review Procedures:

Security Plan Review:

Confirm the commitment to maintain records of all personnel authorized access to protected areas.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Records of all persons authorized access to protected areas are maintained.

### 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.

Source: 73.70(b)

Objective: To control personnel access to vital areas and equipment and maintain information useful for evaluation of potential security-related problems.

Review Procedures:

Security Plan Review:

Confirm the commitment to maintain records of all personnel authorized access to vital areas and vital equipment.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Records of all persons authorized access to vital areas and equipment are maintained.

### 13.7 EMPLOYEE ACCESS

Acceptance Criterion 13.7.A: Establish and maintain a record indicating name, badge number, time of entry, reason for entry and time of exit for all normally unoccupied vital areas.

Source: 73.70(d)

Objective: To control admittance to vital areas and to provide historical information useful for evaluating potential security incidents.

Review Procedures:

Security Plan Review:

Confirm the commitment to maintain a record indicating name, badge number, time of entry and exit, and reason for entry into all normally unoccupied vital areas.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

A record of normally unoccupied vital area entries is maintained which includes name, badge number, time of entry and exit and reason for entry.

### 13.8 NONEMPLOYEE ACCESS

Acceptance Criterion 13.8.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.

Source: 73.50(c)(5), 73.55(d)(6), 73.70(c)

Objective: To control admittance to protected areas and provide historical information useful for evaluation potential security violations.

Review Procedures:

Security Plan Review:

Confirm the commitment to maintaining a register of individuals not employed by the licensee who are granted access to the protected area. Confirm the commitment to require each individual to register his name, date, time, purpose of visit, employment affiliation, citizenship, and individual to be visited.

Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

A register of all nonemployees visiting the facility for any reason is maintained. The register includes name, date, time, purpose of visit, employment affiliation, citizenship and individual to be visited.



## 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. Management of the conduct of physical security audits should be independent of normal physical security management.

Source: 73.55a [Staff requirement based upon the need to provide some assurance that the physical security effectiveness will not be degraded with time].

Objective: To assure the physical security system continues to remain effective and to keep the organization's management continually aware of the emphasis to be placed on security.

#### Review Procedures:

##### Security Plan Review:

Verify that the security plan identifies an organization and specifies the procedures to permit an independent audit of the physical security system at the site. The audit function should include, but not be limited to: review of records to determine completeness and accuracy, interviews with security organization personnel, a check of hardware operability, and simulated security contingencies. Audits should be performed at least once each 12 months. A written audit report should be prepared.

#### Questions and Comments:

Site Visit:

Additional Review:

Evaluation Findings:

Procedures which permit an independent audit of the physical security system are identified. Audits will be performed by \_\_\_\_\_ every \_\_\_\_\_ months. The audit will include \_\_\_\_\_ copies of the audit report with descriptions of any corrective action or modifications to the security system will be located at \_\_\_\_\_.

## APPENDIX A

### Contingencies and Supporting Discussion Requirements

- 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 Perform 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
- 9) Hostage Situation

### Discussion

The criterion is largely derived from 10 CFR 73.55(h)(2). It calls for the development of a plan which will efficiently effect 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.
  - (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.
  - (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.

## APPENDIX A (Continued)

This discussion is not intended to include any actions under any Emergency Plan (Appendix E of 10 CFR Part 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.

## APPENDIX B

### NRR Supplemental Staff Position on Personnel Search Requirements September 30, 1977

The prefatory paragraph of 10 CFR 73.55 as amended September 29, 1977 states that the performance requirements of paragraph (d)(1) as they apply to searches of regular employees of the licensee at the site may be satisfied using only equipment capable of detecting firearms, explosives and incendiary devices. Acceptable metal detector and explosive searching devices of the types currently available are deemed capable of detecting firearms, explosives and incendiary devices for regular employees of the licensee at the site. Such equipment, if not currently in operation, must be purchased and made operational as soon as possible if the licensee using this option is to be in compliance with the performance requirements of 10 CFR 73.55. A regular employee of a licensee is one who is a full time permanent employee whose permanent work station is at the site or those employees of the licensee who report regularly to the site (at least once per week) and includes employees of licensee contractors who are regularly employed at the site. All other personnel\* are required by 10 CFR 73.55 (d)(1) to be searched at points of personnel access to the protected area. The following are acceptable methods for satisfying these requirements:

- (a) A search program consisting of: (1) processing all individuals through an acceptable metal detector, (2) processing all individuals through an explosives search device of the types currently available, (3) conducting a "hands-on" search of at least 5% (selected randomly) of all licensee employees who are not regularly employed at the site, (4) searching a regular employee at the site when the licensee has a well-grounded suspicion that the individual may be carrying firearms, explosives or incendiary devices, with a "hands-on" search, (5) conducting a "hands-on" search of all other individuals, and (6) subjecting all outer garments such as the coats or heavy sweaters of each individual who is not a regular employee at the site to the search requirements at the entry to the protected area.

\*All NRC employees are subject to the search requirements of 73.55 (d)(1). NRC resident inspectors will be searched in the same manner as regular employees of the licensee at the site. Other NRC personnel that have a government granted security clearance will be searched in the same manner as licensee employees who are not regularly employed at the site as long as (1) they can properly identify themselves; and (2) they have been previously identified by the Director of the Regional Office.

#### APPENDIX B (Continued)

The process and procedures which select the individuals to be subjected to a "hands-on" search on a random basis must: (1) require the search to be conducted when the random selection process indicates, regardless of who the person to be searched is, and (2) ensure that an individual entering the search process area cannot know in advance if he or she will be selected for the "hands-on" search.

- (b) For those facilities which have only metal detectors installed and operable, the personnel search program for non-regular employees described in (a)(3) above is acceptable provided that the percentage of individuals randomly selected for "hands-on" search is increased to at least 10%. For those facilities which have only an explosive searching system in operation, the "hands-on" search requirement of (c) below applies.
- (c) For those facilities which have neither metal detectors nor explosives searching devices installed and operable, the personnel search program for non-regular employees described in (a)(3) above is acceptable provided that the percentage of individuals randomly selected for "hands-on" search is increased to at least 20%.

APPENDIX C  
Review Guidelines  
Contents

<u>Guideline</u>	<u>Subject</u>	<u>Page</u>
1	Screening of Individuals Granted Unescorted Access to the Protected Area.....	C-2
2	Escorting of Unattended Visiting Vehicles.....	C-4
3	Performance of Metal Detection Devices.....	C-5
4	Performance of X-Ray Devices.....	C-10
5	Licensee Designated Vehicles.....	C-13
6	Need for Access to Vital Areas.....	C-14
7	(to be issued at a later date)	
8	Criteria for Granting Fewer than 10 Armed Responders.....	C-15
9	Acceptable Compensatory Measures for Intrusion Detection Hardware Outage (e.g., Zone, System) Protected Area Vital Areas.....	C-17
10	Compensatory Measures for the Loss of Normal Power Supply to Security Lighting.....	C-19
11	Vital Area Positive Access Control Definition....	C-20
12	Sabotage Incident Management.....	C-21
13	Compensatory Measures for Vital Areas Lacking the "Two Barrier Protection".....	C-22
14	Locking Systems-Assurance of Safety and Safeguards During an Emergency.....	C-23



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

NOV 26 1977

MEMORANDUM FOR: Reactor Safeguards Licensing Branch Members  
Division of Operating Reactors

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

SUBJECT: SCREENING OF INDIVIDUALS GRANTED UNESCORTED ACCESS  
TO THE PROTECTED AREA "Review Guidelines #1

Screening of individuals granted unescorted access to the protected area helps establish the trustworthiness of employees, prospective employees, and contractors, and reduces the vulnerability of the facility from the threat of an insider. As a minimum, screening programs should meet the guidance in American National Standard, ANSI N18.17, "Industrial Security for Nuclear Power Plants."

In some cases, licensee and contractor employees may not have been subject to the preemployment screening of ANSI N18.17, but the licensee wishes to grant them unescorted access to the protected area. The reason for not using the screening procedures of ANSI N18.17 is that licensee or contractor may have recently implemented a screening program but determined that persons who were employees on the implementation date need not be subject to preemployment screening as a general rule. Also, a licensee or contractor may transfer an employee to a position subject to the screening program but determine the employee need not be subject to the preemployment screening.

Personnel reliability can be adequately established in such cases by a certain minimum length of time of trustworthy employment. This period of trustworthy employment is considered to be equivalent to the reliability established by preemployment screening by ANSI N18.17 and does not decrease the protection of the facility from the threat of the insider.

Based on these considerations, unescorted access to the protected area may be granted to employees of a licensee and its contractors based on the reliability established by three (3) continuous years of trustworthy employment. This method of establishing reliability is considered to be equivalent to the preemployment screening of ANSI N18.17-1973, Sections 4.1 and 4.2. A licensee's program for granting unes-



NOV 26 1977

-2-

corted access to the protected area based on trustworthy employment is acceptable if (a) at least three continuous years of employment of the individual with the licensee or his contractor is documented and (b) the trustworthiness of the individual is determined by a review of the individual's employment record.



Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller  
J. M. Elliott



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

DEC 26 1977

MEMORANDUM FOR: Reactor Safeguards Licensing Branch Members, DOR  
FROM: R. A. Clark, Chief, Reactor Safeguards Licensing Branch, DOR  
SUBJECT: ESCORTING OF UNATTENDED VISITING VEHICLES - REVIEW GUIDELINES #2

The requirement to escort visiting vehicles was included in §73.55 to ensure that an adequate prompt response would be undertaken if a vehicle were used as a weapon against a facility. Escorting of an unattended, visiting vehicle is not needed if adequate alternative measures are taken to assure that the unattended vehicle cannot become such a weapon.

Locking the unattended visiting vehicle and placing the keys in the possession of the security force is adequate to provide assurance that the unattended vehicle cannot become a weapon.

A handwritten signature in dark ink, appearing to read "R. A. Clark", is written over the typed name.

R. A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller  
J. M. Elliott



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

DEC 26 1977

MEMORANDUM FOR: Reactor Safeguards Licensing Branch, DOR

FROM: R. A. Clark, Chief, Reactor Safeguards Licensing Branch, DOR

SUBJECT: PERFORMANCE OF METAL DETECTION DEVICES - REVIEW GUIDELINES #3

All licensees are required to search individuals entering the protected area for firearms. This search is normally conducted by electronic metal detection devices. Enclosed is a standardized procedure that is acceptable to utilize to assure that the metal detectors are operating properly.

A handwritten signature in dark ink, appearing to read "R. A. Clark", is written over the typed name.

R. A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller  
J. M. Elliott

## Performance of Metal Detection Devices

Purpose To assure that the electronic detection devices (metal detectors) are operating properly through appropriate standardized procedures.

General One method to obtain a decrease in the number of false alarms, is to have all personnel remove all metal before going through the device; that is, place all metallic items in a container and pass this container around the detector.

Responsibility The responsibility for assuring and certifying that the detection device meets the minimum detection standard rests with the using facility. The using facility should maintain a record of the calibrations required to maintain the devices in proper working order.

WALK-THROUGH DETECTION DEVICES The objective of a walk-through detection device is the automatic and reliable detection of any hand guns carried by personnel entering protected area. The subject of the search is only the person, not his hand luggage or other hand-carried items. The detection is to be done automatically at walking speed.

### Performance (Calibration) Test

- a. Walk-through detection devices should be set up at a screening station and the sensitivity set to the level or setting that the manufacturer of the device certifies will cause his type of detector to pass the performance test as specified below. It will be necessary to perform the performance test on initial set up of every device. The test should be performed any time a device fails the operational test described below, each time the device is moved, adjusted, and at least quarterly.
- b. The performance test shall consist of passing the following four weapons at the center line of the detection device passageway four times for each of seven orientations and positions specified for a total of 112 tests. A full performance test should take 15 minutes or less to complete. The tester should be devoid of all practical metal including rings, wrist watches, coins, keys, belt buckles, or other metallic objects. The tester should carry each of the specified test weapons at a normal walking speed through the detection device with the gun barrel oriented in the forward, horizontal and vertical positions at the shoulder, waist, and ankle position except in the latter only the vertical orientation should be used, as shown in Figure 1. The overall detection should be at least 95 detections out of the 112 tests. Sensitivity should

be set to achieve 95 out of 112 successive as a minimum.

- c. The test weapons used for calibration are as follows: Colt .25 Automatic, Titan .25 Automatic, General Precision Model 20 .22 LR, and CDM .22 Short.

Operational Test The objective of the operational test is to ensure that the detecting device is maintained in an operable condition.

- a. Each time the device is turned off or maintained it must be tested prior to being used. If the unit is never turned off, it must be tested at least once every seven days.
- b. The operational test should consist of passing the CDM 22 short weapon held horizontal at the waist three times through the device in the direction of traffic flow through the detector. The detector should signal the presence of the weapon on at least two of the three passes.

HAND-HELD DETECTION DEVICES Detection is indicated by a squealing sound from a loud speaker within the unit when the unit is brought into the vicinity of metal. A squeal will be heard when the unit passes over metal. A high squeal indicates a greater mass of metal is presented.

CALIBRATION PROCEDURES FOR HAND-HELD DEVICES Devices in present use should be calibrated in accordance with manufacturer's instructions.

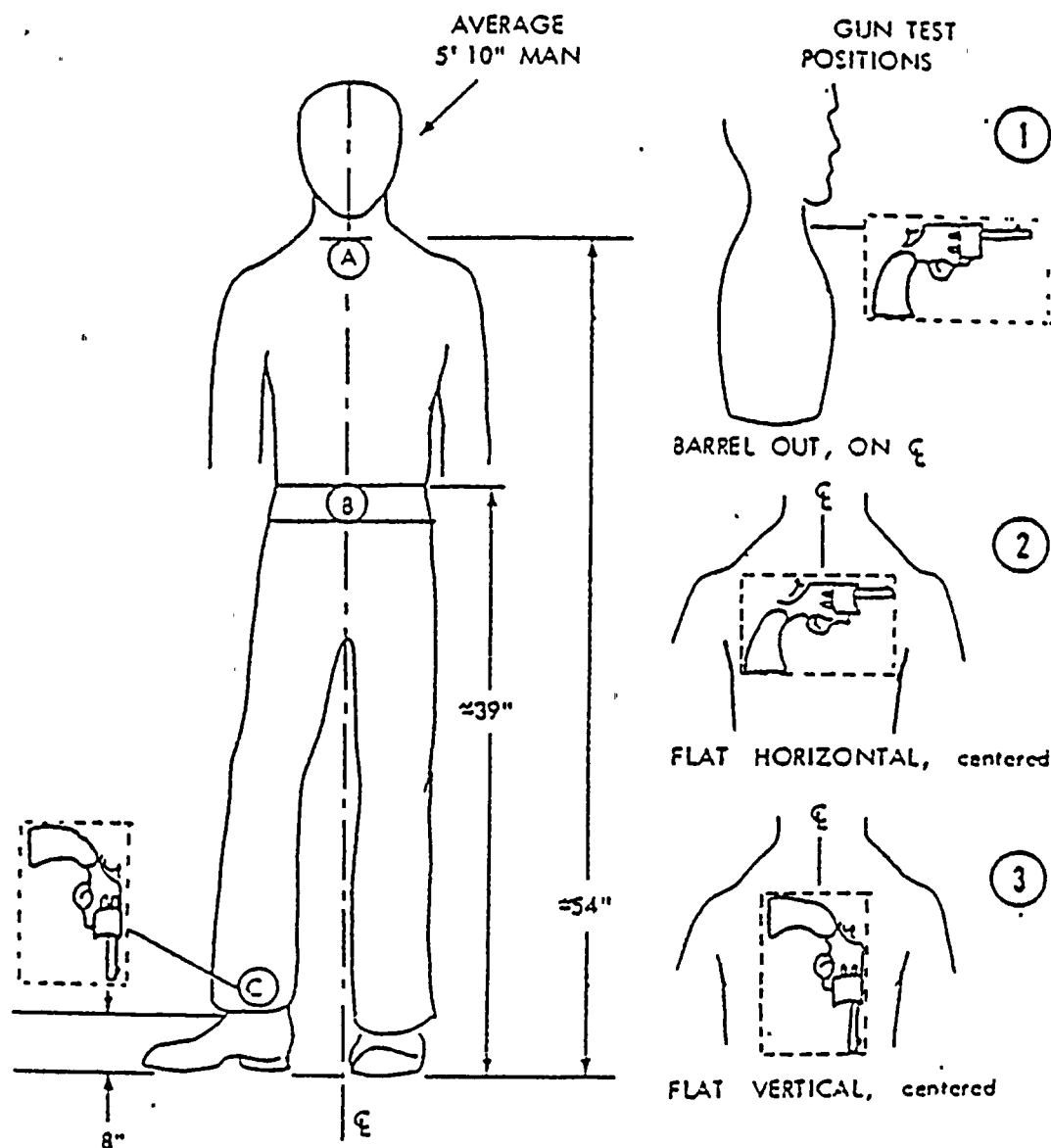
SUGGESTED SEARCH PROCEDURES FOR THE USE OF ALL HAND-HELD DEVICES  
The following procedures should be used in conducting a search using hand-held detection devices.

- a. Assure that the detection device is in proper working order.
- b. With the device approximately two to four inches from the subject, slowly pass the device over the entire body with the detection loop parallel with the body, front and back. Then pass the device slowly over the arms and legs, front, back and sides. Particular attention should be paid to waist, groin, armpit, and ankle area. With practice, a thorough search can be made in one minute. Hand-carried outer garments will be searched by hand. Bags and parcels of any size will not be searched using a hand-held weapon detection device.
- c. If unit alarms, it indicates that metal is present in a given area. Ask subject to remove any metal and search again.

Performance Test The performance test for hand-held detectors should be conducted at the beginning of each shift: The CDM .22 short will be placed in positions 1 through 3 as shown in Figure 1. The detection

should be at least 3 detections out of 3 tests for each position tested.

Operational Test The operational test for hand-held metal detectors is the same as the performance test.



PLANT GUNS IN LOCATION A, B, C, AS FOLLOWS:

- Loc A: Position 1, 2, and 3 with top edge of box as shown by locating dimension.
- Loc B: Position 1, 2, and 3 with top edge of box as shown by locating dimension.
- Loc C: Position 3 with bottom edge of box as shown by locating dimension.

Figure 1



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

DEC 20 1977

MEMORANDUM FOR: Reactor Safeguards Licensing Branch, DOR  
FROM: Robert A. Clark, Chief, Reactor Safeguards  
Licensing Branch, DOR  
SUBJECT: PERFORMANCE OF X-RAY DEVICES - REVIEW GUIDELINES #4

All licensees are required to search packages entering the protected area. This search may be conducted by X-ray devices. Enclosed is a standardized procedure that is acceptable to assure the X-ray devices are operating properly.

A handwritten signature in cursive script, reading "Robert A. Clark", is positioned above the typed name and title.

Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller  
J. M. Elliott



## Performance of X-Ray Devices

### Equipment Performance Standard:

- (1) An X-ray monitor must be able to image and an operator must be able to see an insulated 24 gauge solid copper wire.

### Operator Performance Standard:

- (1) Operators of an X-ray monitor must be trained to recognize unauthorized articles, including weapons, explosives and incendiary devices in X-ray images.

### X-ray Imaging Testing:

- (1) At least quarterly, each X-ray system shall be tested to assure that the monitor will image and an operator can see insulated 24 gauge solid copper wire.
- (2) A wire test kit is used consisting of samples of 20, 22, 24 and 26 gauge solid copper wire.
- (3) The wire test samples are placed in X-ray systems in the same way packages are introduced. If the 26 gauge wire can be seen, the X-ray exceeds performance standards. If the 24 gauge wire can be seen clearly, the X-ray is acceptable. If 22 gauge wire can be seen clearly but not 24 gauge, the X-ray monitor must be repaired or replaced within 48 hours. If 20 gauge wire can be seen but not 22 or 24 gauge, the X-ray monitor must be repaired

or replaced within 24 hours. If 20 gauge wire cannot be seen, the X-ray cannot be used for the screening of packages. Items must be physically inspected.

X-ray Operator Testing:

- (1) An evaluation of operator performance is conducted at least quarterly at each X-ray system. The procedures set forth below are followed using as the test object guns designed for calibration of detector testing. (COLT .25 automatic, Titan .25 automatic, General Precision Model 20.22LR, CPM.22 cal.)
- (2) The test object is positioned in a package so that a clear undisguised lateral (profile) image would logically be projected on the monitor during X-ray inspection of the package.
- (3) The person conducting the test presents the package for inspection just as any person would - without prior notification or identification.
- (4) If the operator detects the object, he or she is appropriately credited.
- (5) If the test object is visible on the monitor and is not detected by the operator, arrangements are made for corrective action such as training, supervision, disciplinary action, etc.
- (6) If a clear image of the test object is not visible on the X-ray monitor, the wire test is conducted to make certain the X-ray is operating satisfactorily. If it is, the operator test is repeated. If not, appropriate corrective action is taken.



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

DEC 26 1977

MEMORANDUM FOR: Reactor Safeguards Licensing Branch, DOR  
FROM: R. A. Clark, Chief, Reactor Safeguards  
Licensing Branch, DOR  
SUBJECT: LICENSEE DESIGNATED VEHICLES - REVIEW GUIDELINES #5

Licensee Designated Vehicles are defined as those vehicles that are limited in their use to onsite plant functions and remain in the protected area except for operational, maintenance, repair, security and emergency purposes. These vehicles can be used by only authorized persons for authorized purposes. These vehicles shall be locked and the ignition key removed when unattended.

These vehicles will only be allowed to leave the protected/owner-controlled area for the purpose of servicing, repairs, emergencies or other directly related activities. Under these circumstances, a search of the vehicle will be conducted prior to reentry.

After the initial search, licensee designated vehicles may be allowed to leave the protected area and return without being searched providing:

1. The vehicle did not leave the owner-controlled area.
2. Two individuals having unescorted access to the protected area have been with the vehicle continuously to insure the vehicle is not being used to transport weapons, explosives or incendiary devices into the protected area.

A handwritten signature in dark ink, appearing to read "R. A. Clark", is written over the typed name and title.

R. A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller  
J. M. Elliott



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

DEC 20 1977

MEMORANDUM FOR: Reactor Safeguards Licensing Branch, DOR

FROM: R. A. Clark, Chief, Reactor Safeguards  
Licensing Branch, DOR

SUBJECT: NEED FOR ACCESS TO VITAL AREAS - REVIEW GUIDELINE #6

Positive access control is required for the physical protection of nuclear power plants. Positive access control provides assurance that only authorized individuals enter a vital area for authorized reasons. One element of positive access control is the establishment of the need for access. A system for establishing the need for access should be based on an individual's assigned duties and normal working hours. During normal working hours an individual should be granted access based upon his position. It is not necessary to determine his exact reason to enter a vital area that is associated with his assigned tasks. During times other than normal working hours an individual should confirm a need to enter a vital area. The following describes an acceptable method of establishing a need for access to vital areas.

Need for Access

- (1) The need for access is established when an individual is authorized access to vital areas. This need for access is revalidated at least once every 31 days. During normal working hours, an individual is granted access to those vital areas identified in his authorization.
- (2) The shift supervisor is notified of all individuals on site more than one hour after the end of the individual's normal working hours. No further action is required unless directed by the shift supervisor.
- (3) The shift supervisor is notified prior to granting an individual access to the protected area at times other than the individual's normal reporting time. When granting access to the protected area, the shift supervisor may also grant access to those vital areas identified in the individual's authorization.

  
R. A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller  
J. M. Elliott



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

DEC 26 1977

MEMORANDUM FOR: Reactor Safeguards Licensing Branch, DOR

FROM: R. A. Clark, Chief, Reactor Safeguards  
Licensing Branch, DOR

SUBJECT: CRITERIA FOR GRANTING FEWER THAN 10 ARMED  
RESPONDERS - REVIEW GUIDELINE #8

The regulations provide for a nominal number of armed response personnel as ten (10) and that this number may not be reduced to less than five (5) guards. The statement of consideration states that the number of such personnel may be more or less than the nominal number depending on factors such as the following, to be considered during evaluation of a licensee's physical security plan, not necessarily in order of importance:

- (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 LLEA response.
- (g) Vital area hardening, including plant design, location of and access control to vital areas.
- (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.

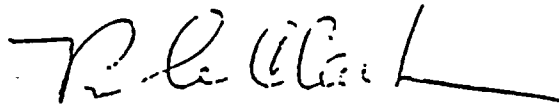
In addition to these criteria, the following factors may be considered to evaluate the case by case justification for response personnel numbers:

- (a) The LLEA response time and their numbers.
- (b) The quality of the screening program.
- (c) The complexity of the layout of the plant within the protected area.
- (d) The analysis of the integrated security system as described in NUREG 0220, Chapter 11.

Reactor Safeguards Licensing  
Branch

-2-

- (e) Factors outside the owner controlled area that may increase or decrease the vulnerability of the protected area and are beyond the licensee's control.
- (f) The availability of guards or response personnel from other guard forces in the vicinity.



R. A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors

cc: J. R. Miller  
J. M. Elliott



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

JAN 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch Members, DOR

FROM: Robert A. Clark, Chief, Reactor Safeguards  
Licensing Branch, DOR

SUBJECT: ACCEPTABLE COMPENSATORY MEASURES FOR INTRUSION DETECTION  
HARDWARE OUTAGE (E.G., ZONE, SYSTEM) PROTECTED AREA  
VITAL AREAS - REVIEW GUIDELINE NUMBER 9

The objective of perimeter intrusion detection hardware is to detect the unauthorized entry or attempted entry of individuals or vehicles into the protected area and to provide an "alert" to the security organization so that response by a response force will be initiated at the time of penetration into the protected area.

In the event of a hardware outage the compensatory measures must satisfy this objective by providing a means for detecting unauthorized entry and for alerting the security organization or by providing a response force to control all paths from the area of outage to all vital areas. Acceptable measures compensatory to perimeter intrusion detection outage are:

- a) Back-up intrusion detection system of equal capability.
- b) Dedicated CCTV with continuous monitoring of the perimeter zone(s) affected by the outage.
- c) On-the-spot guards visually monitoring the perimeter zone(s) affected by the outage.
- d) Response force deployed to control all paths from the perimeter zone(s) affected by the outage to all vital areas.

The objective of the vital area intrusion detection hardware is to detect the unauthorized entry of individuals (and at some facilities - vehicles) into vital areas and to provide to the security organization an "alert" so that response by a response force will be initiated at the time of penetration into the vital area.

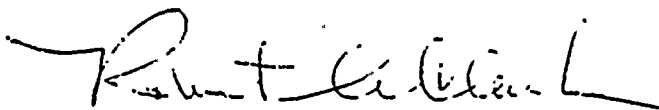
In the event of a hardware outage the compensatory measures must satisfy this objective by either providing a means for detecting unauthorized

Reactor Safeguards Licensing  
Branch Members

-2-

entry and alerting the security organization or providing the response force to control the paths to the affected vital areas. Acceptable measures compensatory to a vital area intrusion detection outage are:

- a) A back-up intrusion detection system of equal capability.
- b) Dedicated CCTV with continuous monitoring of the portals affected by the outage.
- c) On-the-spot guards visually monitoring the portals affected by the outage.
- d) Response force deployment to control all approaches to the affected vital areas.



Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch  
Division of Operating Reactors





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

JAN 10 1978

File

MEMORANDUM FOR: Reactor Safeguards Licensing Branch


FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

SUBJECT: COMPENSATORY MEASURES FOR THE LOSS OF NORMAL  
POWER SUPPLY TO SECURITY LIGHTING - REVIEW  
GUIDELINE NUMBER 10

Illumination, as an element of a security system, provides a security organization with the capability to visually monitor the protected area to permit early detection and assessment and to a limited extent acts as a deterrent to potential intruders. Upon the loss of this element, certain compensatory measures must be implemented to counteract the deficiencies.

The following represent some of the acceptable compensatory measures which when utilized separately or in combination, would be found appropriate:

- 1) Switch to stand-by power.
- 2) Low light level surveillance devices.
- 3) Portable lighting devices.
- 4) Positioning of security personnel at strategic locations for adversary interception.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch



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

JAN 11 1978


MEMORANDUM FOR: Reactor Safeguards Licensing Branch

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

SUBJECT: VITAL AREA POSITIVE ACCESS CONTROL DEFINITION -  
REVIEW GUIDELINE NUMBER 11

Positive Access Control is defined as those measures necessary to assure that individuals who request entry into vital areas have been determined to have a need for such access and that these individuals have been positively identified before entry is granted into those areas.

For vital areas, positive access control is accomplished upon entry into the Protected Area where personnel are positively identified as having a need for access and "keys" are issued for vital areas according to the assessed need.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing  
Branch



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

JAN 16 1976

MEMORANDUM FOR: Reactor Safeguards Licensing Branch

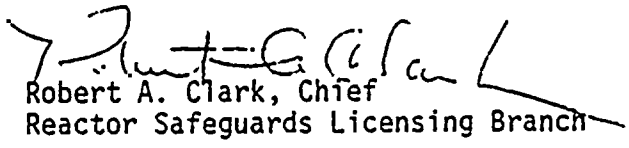
FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

SUBJECT: SABOTAGE INCIDENT MANAGEMENT - REVIEW GUIDELINE  
NUMBER 12

The licensee is responsible for the safe operation of his nuclear power plant and therefore is obligated to employ effectively all resources within his control to protect the public health and safety under all circumstances, including a sabotage incident.

The security plans and procedures implementing the security plans prescribe the means to provide protection with high assurance against successful industrial sabotage by two design level threats (§73.55 (a)(1)(2)). The protection thus afforded is not limited to the design level threats, but will also provide a lesser or greater degree of protection for threats that are larger or smaller, simpler or more sophisticated.

In the event of a sabotage attempt, the available licensee and LLEA resources and forces must be used in the most effective manner to counter the actual threat based on the circumstances of the situation. It is recognized that the Security Plan and the implementing security procedures may not equally or adequately address the complete range of possible threats. Therefore, it is necessary that the security plan and procedures accommodate the necessary freedom of action needed by the individual in charge at the site at time of an actual threat to employ the available resources (e.g. physical protection systems, security organization, response forces, LLEA, etc) in a manner that he considers most effective to counter that threat.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch



F.1E

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

JAN 10 1978

MEMORANDUM FOR: Reactor Safeguards Licensing Branch

FROM: Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

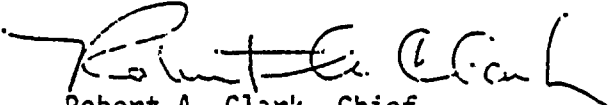
SUBJECT: COMPENSATORY MEASURES FOR VITAL AREAS LACKING  
THE "TWO BARRIER PROTECTION" - REVIEW GUIDELINE  
NUMBER 13

10 CFR 73.55 requires that vital equipment be protected by a minimum of two barriers i.e., Protected and Vital, which are defined in 10 CFR 73.2. The barriers coupled with the defense in depth concept, isolation zones, continuous monitoring and periodic surveillance result in high assurance detection and resistance to penetration.

In some cases barrier separation is impossible to achieve due to operational design needs, as exemplified most often by the positioning of the service water intake structures on borders of bodies of water. In other cases location of vital equipment was instituted prior to the issuance of 73.55, making it impractical to require relocation. In both cases other measures must be implemented to compensate for the loss of the basic criteria.

The following represent some acceptable compensatory (or equivalent) measures that may be used together or separately (depending upon site specifics) in achieving the objective:

1. Hardening of common barriers.
2. Additional "early warning" monitoring devices.
3. More frequent surveillance.
4. Positive response posture to common barrier locations.
5. Positioning of security post in close proximity of common barriers.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch



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

NO 1 1 7 7 7 7

MEMORANDUM FOR: Reactor Safeguards Licensing Branch

FROM: R. A. Clark, Chief  
Reactor Safeguards Licensing Branch


SUBJECT: LOCKING SYSTEMS-ASSURANCE OF SAFETY AND SAFEGUARDS  
DURING AN EMERGENCY-REVIEW GUIDELINE NUMBER 14

Under emergency conditions, prompt ingress into certain safety-related areas must be assured to enable safe shutdown of a nuclear power plant, and unimpeded egress from all parts of the facility must be assured in the interest of personnel safety.

The design and operation of security devices for doors to vital areas should be based on both safety and security. The following provides guidance on the design and use of security devices on vital area doors:

- a) Prompt emergency ingress into electrically and mechanically locked-safety-related areas by essential personnel must be assured in any postulated occurrence through the combined use of the features below or, the equivalent.
  - 1) Provide reliable and uninterruptable auxiliary power to the entire electrical locking system, including its controls (sufficient physical separation, electrical isolation, and redundancy must be provided to prevent the occurrence of a common mode failure in the uninterruptable auxiliary power supply for the lock system in any design basis event); and
  - 2) Provide electrical locking devices which fall in the secure mode upon loss of both primary and auxiliary power and are equipped with secure mechanical means and associated procedures to override the failed electrical locking devices (e.g., key locks with keys held by appropriate personnel who know when and how to use them); or
  - 3) Provide electrical locking devices which fail in the open mode upon loss of both primary and auxiliary power and associated procedures which provide compensatory measures for the open doors (e.g., deploying guards to strategic points)

- (The fail open feature should be used only on selected interior doors.); or
- 4) Provide key locks with keys held by appropriate personnel who know when and how to use them; and
  - 5) Provide periodic testing of all locking systems and mechanical overrides to confirm their operability under auxiliary power as well as failed conditions.
- b) Unimpeded emergency egress must be assured from all parts of facilities, the security hardware and systems must be designed and installed so as to not degrade personnel safety, and such hardware and systems should be in conformance with applicable (State/Local) fire regulations and life safety codes.

  
Robert A. Clark, Chief  
Reactor Safeguards Licensing Branch

Washington Public Power Supply System

CCS:

Joseph B. Knotts, Jr., Esq.  
Debevoise & Liberman  
700 Shoreham Building  
806 Fifteenth Street, N. W.  
Washington, D. C. 20005

Richard Q. Quigley, Esq.  
Washington Public Power Supply System  
3000 George Washington Way  
P. O. Box 968  
Richland, Washington 99352

Nepom & Rose  
Suite 101 Kellogg Building  
1935 S. E. Washington  
Milwaukie, Oregon 97222

Ms. Helen Vozenilek  
7214 S. E. 28th Street  
Portland, Oregon 97202

Ms. Susan M. Garrett  
7325 S. E. Steele Street  
Portland, Oregon 94206

Nicholas Lewis, Chairman  
Energy Facility Site Evaluation Council  
820 East Fifth Avenue  
Olympia, Washington 98504