



I 28

South

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555
February 10, 1977

MEMORANDUM FOR: Upgrade Working Group

FROM: L. J. Evans, Jr., Chief
Requirements Analysis Branch

SUBJECT: STATUS REPORT--UPGRADE RULE ACTIVITY

Consistent with decisions made at the February 1 working group meeting and our earlier scoping of the safeguard upgrade rule effort, work is proceeding to develop alternative approaches to implementing the upgrade. At present, three options appear to be viable. First, a totally performance-oriented rule. Second, a rule which includes both performance requirements and detailed systems specifications, which are not integrated. Third, a rule which includes and integrates both performance requirements and minimum essential system specifications. *Does not match the attachment.*

Attached please find examples of drafts which should be useful for developing the third option. The attachments include narratives of the first three basic capabilities which have been developed by A. Poltorak and a write-up of minimum essential safeguard system specifications which have been developed by D. Kasun. Obviously, these have not been integrated yet. However, work has begun to show how such integration would be accomplished. All of the attached drafts are in early stages of development and therefore numerous changes are anticipated and comments by working group members would be appreciated. As you review the basic capability documents, it would be helpful if you would organize your comments under the following categories: (1) Are all sections and entries complete? (2) Are the sections organized logically? (3) Does the narrative say what it was meant to say?

Review of the tasks delineated in the safeguards working group responsibilities chart which was forwarded to you by memorandum of January 24, 1977, shows those tasks to have the following status.

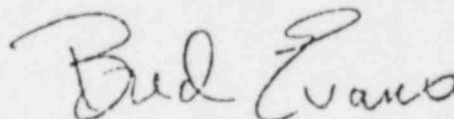
Upgrade Working Group

2

February 10, 1977

<u>Task</u>	<u>Task Leader</u>	<u>Immed Prod Due</u>	<u>Status</u>
o Formulate Performance Oriented Specifications	Poltorak	1/28	Drafts submitted
o Formulate Minimum Safeguards System Specifications	Kasun	1/28	Draft submitted
o Integrate Performance-Oriented Specifications & Minimum Safeguards System Specifications	Poltorak	1/28	2 weeks slippage
o Formulate Regulatory Design Guidance	Michaels	2/8	Draft submitted
o Insure GESMO Safeguards Supplement Consistency	Hatter	2/4	1 week slippage
o Insure NRR 73:55 Consistency	Miller	2/15	On schedule
o Develop Upgrade Guides & Technical Reports	Jones	2/28	On schedule
o Develop License Review Plans	Levy	2/28	On schedule
o Develop Site Assessment Procedures	South	3/1	On schedule

Finally, a working group meeting will be held on Friday, February 18. Therefore, please submit your comments on the attached drafts by c.o.b. Wednesday, February 16, so that we can compile them and give copies to all members of the working group for use during that meeting. We will call early next week to schedule the time and place.


L. J. Evans, Jr.

Attachment

DISTRIBUTION:

Upgrade Working Group

O. Chambers (IE)
R. Jones (SD)
T. Michaels (SD)
R. Fonner (ELD)
Mike Smith (SG)
D. Kasun (SG)
C. South (SG) ✓
B. Hatter (SG)
A. Poltorak (SG)
John J. Miller (NRR)
B. Nulsen (SG)

Information List

R. Page (SG)
B. Erickson (SG)
J. Powers (SG)
R. Brightsen (SG)
E. Perchonok (SG)
F. Arsenault (RES)
M. Elliott (NRR)
N. Haller (IE)
T. Sherr (SG)
E. McAlpine (SG)
F. Crane (SG)
D. Sutton (SG)
D. Kunihiro (SG)
J. Prell (SD)
R. Ramirez (SD)

Basic Capability 1 Narrative

The safeguard system shall provide the capabilities to prevent unauthorized personnel entry and prevent introduction of unauthorized material into MAA's and VA's. The licensee must provide access control systems that are able to detect unauthorized attempts to gain access by persons and detect attempts to introduce unauthorized material in sufficient time to permit an effective and acceptable response. ~~which prevents unauthorized personnel entry and introduction of unauthorized material.~~

The following safeguard subsystems are ^{a minimum} necessary to assure the ^{required} detection capability. (See Section ___ for necessary aspects of the response capability.)

A. To detect attempts to gain ^{unauthorized} access or introduce material by stealth across MAA and VA boundaries, the following are needed:

1. Access Detection Systems: The licensee shall provide detection systems and procedures that, ^(need to define) in a timely manner, will:

a.) detect and annunciate to the reaction and/or response forces any access or penetration ^{the MAA or VA boundaries} attempts by persons or of material;

b.) collect sufficient information for assessment of adversary characteristics and intent;

c.) assess the information; and

d.) appropriately communicate ^{the assessment result to} with reaction and response forces.

2. Barriers: The licensee shall provide barriers that will:

a.) channel casual penetration of persons and material to MAA and VA Entry Controls; and

b.) delay penetration attempts by persons and introduction of material sufficiently to permit the detection and response systems to function in an effective manner. (See Section —).

B. To detect attempts to gain access by deceit into MAA's and VA's, the following are needed:

1. Access Authorization Controls: The licensee shall provide authorization controls and procedures for personnel and material entry that will:
 - a.) establish updated entry requirements; *← defines*
 - b.) establish accurate authorization schedules based on routine operational and non-routine/emergency requirements.
2. Entry Controls: The licensee shall provide entry controls and procedures to:
 - a.) verify the identity of persons presenting themselves for access and/or material presented for introduction;
 - b.) assess the verified identity and/or material against the authorization schedules and entry requirements; *to establish validity* and
 - c.) appropriately interface with reaction forces. *to permit entry or take corrective action.*

Basic Capability 2 Narrative

The safeguard system shall provide the capabilities to prevent unauthorized activities and unauthorized conditions within PA's, VA's, and MAA's. The licensee must provide activity and condition control systems that are able to detect unauthorized activities and unauthorized conditions in sufficient time to permit an effective and acceptable response. ~~which prevents unauthorized activities and unauthorized conditions to exist or continue.~~

Safeguard's subsystems are a minimum
The following ~~functions are required of the safeguard system to~~ assure the detection capability. (See Section ___ for required functions of the response capability.)

A. To detect unauthorized activities or unauthorized conditions within PA's, VA's, and MAA's, the following are needed:

1. Authorization Controls: The licensee shall provide authorization controls and procedures that will establish the activities and conditions permitted within each of the areas with unique requirements. *(not clear what this means)*

2. Boundaries: The licensee shall define boundaries for the areas that have unique requirements *(need to define)* for authorized activities and conditions.

3. Activity and Condition Detection Systems: The licensee shall provide detection systems and procedures that, *(need to define)* in a timely manner, will:

a.) surveil, monitor and/or inspect each of the defined areas to discover activities and conditions that are not authorized;

b.) collect sufficient information for assessment of the nature of the activity and/or condition;

c.) assess the information; and

d.) *the assessment result to* appropriately communicate ~~with~~ reaction/response forces.

Basic Capability 3 Narrative

The safeguard system shall provide the capabilities to prevent unauthorized and unconfirmed removal of SNM from MAA's. The licensee must provide removal control systems that are able to detect unauthorized attempts to remove SNM in sufficient time to permit a response, confirm that SNM is being removed in an authorized manner, and provide an effective and acceptable response, ~~which prevents unauthorized and unconfirmed removal of SNM.~~

The following safeguard subsystems ^{a minimum} are ~~necessary~~ to assure the detection and confirmation capabilities. (See Section ___ for necessary aspects of the response capability.)

A. To detect attempts at unauthorized removal of SNM by stealth from MAA's, the following are needed:

1. Removal Detection Systems: The licensee shall provide detection systems and procedures that, in a timely manner, will:
 - a.) detect and annunciate to the reaction and/or response forces any attempts to remove SNM;
 - b.) collect sufficient information for assessment of removal attempt characteristics;
 - c.) assess the information; and
 - d.) ~~appropriately~~ ^{the assessment result to} communicate ~~with~~ reaction and response forces.
2. Barriers: The licensee shall provide barriers that will:
 - a.) channel exit attempts to exit controls;
 - b.) delay any attempts to remove SNM sufficiently to permit the detection and response systems to function in an effective manner. (See Section _____).

B. To detect attempts at unauthorized removal of SNM by deceit from MAA's, the following are needed:

1. Removal Authorization Controls: The licensee shall provide authorization controls and procedures that will establish accurate properties for authorized removal of SNM by specifying the characteristics of the SNM authorized for removal, the person(s) authorized to remove the SNM, and the removal schedule.
2. Removal Controls: The licensee shall provide removal controls and procedures that will:

- a.) determine the apparent characteristics of the SNM presented for removal;
- b.) verify the identity of the person(s) presenting the SNM for removal;
- c.) verify the removal schedule;
- d.) assess the apparent SNM characteristics and the verified identity and removal schedule against the authorized removal properties; *to establish validity* and
- e.) appropriately interface with the SNM Confirmation Controls and/or reaction forces. *to permit removal or take corrective action*

C. To confirm the identity of SNM presented for authorized removal from MAA's, the following is needed:

1. SNM Confirmation Controls: The licensee shall confirm the authorized removal of SNM by providing controls and procedures that will:
 - a.) verify the apparent characteristics of the SNM presented for removal;

b.) assess the confirmed SNM characteristics against the author
to establish validity
characteristics; and

c.) appropriately interface with the reaction force. *to permit*
removal or take corrective action.

J. J. Kasun
2/4/77

SAFEGUARDS UPGRADE RULE

Minimum Essential Requirements

A. Security Organization

- (1) A security organization including a guard force having the size, armament, equipment, deployment and training capable of ~~clearly~~ defeating the design basis violent assault without outside assistance.
- (2) Liaison with LLEA to insure (i) rapid apprehension (offsite) of attackers (ii) execution of powers of arrest and (iii) assistance against assaults larger than the design basis event.

Accompanying Guides

- Guard force armament, equipment and training
- Guard force size and operation
- Liaison with LLEA

B. Barrier Protection

- (1) A ^{defined} system of barriers to ^{define} delay or deny entrance by personnel and vehicles into the protected area, vital areas and material access areas.
- (2) Penetration ^{defined} resistant vaults for storage and protection of high quality SNM.
- (3) Structures containing alarm, control and defensive positions hardened to prevent penetration by the design basis weapons.
- (4) Area denial systems to protect SNM in process (non-lethal debilitating vapors or liquids)

Accompanying Guides

- Barrier Design
 - PA, VA and MAA (general)
 - Vehicle barriers
 - Vaults
 - Hardening of alarm and control stations
 - Defensive Positions
- Area Denial Systems

C. Communications

- (1) Capability for continuous radio voice communication between the guard force and alarm and control stations and between the facility and LLEA. *(Multi-channel or secure, non secure or encrypted communications, etc.)*
- (2) A facility wide tamper-indicating duress alarm system linked to LLEA *(land line only?)*

Accompanying Guides

- Communications System
- Duress alarm system

D. Intrusion Alarm System

- (1) An ~~electronic~~ ^(define) tamper-indicating alarm system for high assurance detection of unauthorized entry (i) into a protected area and (ii) into or within vital areas and material access areas.
- (2) A system for rapid ^(define) assessment of (i) a perimeter or interior alarm, and (ii) the nature and extent of ~~a threat~~ ^{the intrusion} (this includes clear areas, illumination, emergency lighting and CCTV).

- (3) Duplicate independent alarm and control stations

Associated Guides

- Perimeter Intrusion Alarm Systems
- Interior Intrusion Alarm Systems
- Alarm and control stations
- Alarm Assessment

E. Control of Entry and Exit

- (1) A system, including access controls and search of personnel, vehicles, packages and material, to prevent unauthorized entry of personnel, vehicles, weapons and explosives into the protected area, vital areas and material access areas.

STATIONS
is
?

Implies no hierarchy of commands. Also not necessarily interconnected.
Functionally or physically duplicate?
Should be specific in what is meant.
Word "independent" should be changed to "not dependent".

- (2) A system, including search of personnel, vehicles, packages and material exiting a material access area, to prevent unauthorized removal of SNM.
- (3) Special containment of high quality, divertible size SNM including isolation of work areas, limited access, surveillance of employees and restrictions on personal articles and clothing (this includes a prohibition against the wearing of metal bearing clothing and the carrying of metal objects thru the material access area exit point.) *(define)*

Accompanying Guides

- Access controls
- Search Techniques and Equipment

F. Testing

- (1) A system, including frequent functional tests, to insure that security equipment sub-systems are operating properly. *(define)*
- (2) A system to insure that the performance of security organization personnel is adequate. *(define)*
- (3) A procedure for the integrated testing of the overall facility safeguards system. *(frequency?, evaluation criteria, and success criteria)*
- (4) A plan for testing the LLEA response capabilities *(frequency?)*

Accompanying Guides

- Alarm System and Communications Testing
- Performance Testing of Security Personnel
- Safeguards System Testing
- Verification of LLEA Response



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555
February 10, 1977

*Page 2/13/77
L. J. Evans*

I've written in several comments. Time is rapidly passing so this activity must be accelerated if you are to meet the target date for completion.

MEMORANDUM FOR: Upgrade Working Group
FROM: L. J. Evans, Jr., Chief
Requirements Analysis Branch
SUBJECT: STATUS REPORT--UPGRADE RULE ACTIVITY

Consistent with decisions made at the February 1 working group meeting and our earlier scoping of the safeguard upgrade rule effort, work is proceeding to develop alternative approaches to implementing the upgrade. At present, three options appear to be viable. First, a totally performance-oriented rule. Second, a rule which includes both performance requirements and detailed systems specifications, which are not integrated. Third, a rule which includes and integrates both performance requirements and minimum essential system specifications.

Attached please find examples of drafts which should be useful for developing the third option. The attachments include narratives of the first three basic capabilities which have been developed by A. Poltorak and a write-up of minimum essential safeguard system specifications which have been developed by D. Kasun. Obviously, these have not been integrated yet. However, work has begun to show how such integration would be accomplished. All of the attached drafts are in early stages of development and therefore numerous changes are anticipated and comments by working group members would be appreciated. As you review the basic capability documents, it would be helpful if you would organize your comments under the following categories: (1) Are all sections and entries complete? (2) Are the sections organized logically? (3) Does the narrative say what it was meant to say?

Review of the tasks delineated in the safeguards working group responsibilities chart which was forwarded to you by memorandum of January 24, 1977, shows those tasks to have the following status.

Copy of 82-208767

<u>Task</u>	<u>Task Leader</u>	<u>Immed Prod Due</u>	<u>Status</u>
o Formulate Performance Oriented Specifications	Poltorak	1/28	Drafts submitted
o Formulate Minimum Safeguards System Specifications	Kasun	1/28	Draft submitted
o Integrate Performance-Oriented Specifications & Minimum Safeguards System Specifications	Poltorak	1/28	2 weeks slippage
o Formulate Regulatory Design Guidance	Michaels	2/8	Draft submitted
o Insure GESMO Safeguards Supplement Consistency	Hatter	2/4	1 week slippage
o Insure NRR 73:55 Consistency	Miller	2/15	On schedule
o Develop Upgrade Guides & Technical Reports	Jones	2/28	On schedule
o Develop License Review Plans	Levy	2/28	On schedule
o Develop Site Assessment Procedures	South	3/1	On schedule

Finally, a working group meeting will be held on Friday, February 18. Therefore, please submit your comments on the attached drafts by c.o.b. Wednesday, February 16, so that we can compile them and give copies to all members of the working group for use during that meeting. We will call early next week to schedule the time and place.

Bed Evans
L. J. Evans, Jr.

Attachment

DISTRIBUTION:

Upgrade Working Group

O. Chambers (IE)
R. Jones (SD)
T. Michaels (SD)
R. Fonner (ELD)
Mike Smith (SG)
D. Kasun (SG)
C. South (SG)
B. Hatter (SG)
A. Poltorak (SG)
John J. Miller (NRR)
B. Nulsen (SG)

Information List

R. Page (SG) ✓
B. Erickson (SG)
J. Powers (SG)
R. Brightsen (SG)
E. Perchonok (SG)
F. Arsenault (RES)
M. Elliott (NRR)
N. Haller (IE)
T. Sherr (SG)
E. McAipine (SG)
F. Crane (SG)
D. Sutton (SG)
D. Kunihiro (SG)
J. Prell (SD)
R. Ramirez (SD)

Basic Capability 1 Narrative

The safeguard system shall provide the capabilities to prevent unauthorized personnel entry and prevent introduction of unauthorized material into MAA's and VA's. The licensee must provide access control systems that are able to detect unauthorized attempts to gain access by persons and detect attempts to introduce unauthorized material in sufficient time to permit an effective and acceptable response which prevents unauthorized personnel entry and introduction of unauthorized material.

The following safeguard subsystems are necessary to assure the detection capability. (See Section ___ for necessary aspects of the response capability.)

A. To detect attempts to gain access or introduce material by stealth across MAA and VA boundaries, the following are needed:

1. Access Detection Systems: The licensee shall provide detection systems and procedures that, in a timely manner, will:

- a.) detect and annunciate to the reaction and/or response forces any access or penetration attempts by persons or of material;
- b.) collect sufficient information for assessment of adversary characteristics and intent;
- c.) assess the information; and
- d.) appropriately communicate with reaction and response forces.

2. Barriers: The licensee shall provide barriers that will:

- a.) channel casual penetration of persons and material to MAA and VA Entry Controls; and

*Be caught here
This must be
...
...
...
in their plants*

*to those
→
...*

...

b.) delay penetration attempts by persons and introduction of material sufficiently to permit the detection and response systems to function in an effective manner.

B. To detect attempts to gain access by deceit into MAA's and VA's, the following are needed:

1. Access Authorization Controls: The licensee shall provide authorization controls and procedures for personnel and material entry that will:

- a.) establish updated entry requirements;
- b.) establish accurate authorization schedules based on routine operational and non-routine/emergency requirements.

2. Entry Controls: The licensee shall provide entry controls and procedures to:

- a.) verify the identity of persons presenting themselves for access and/or material presented for introduction;
- b.) assess the verified identity and/or material against the authorization schedules and entry requirements; and
- c.) appropriately interface with reaction forces.

The safeguard system shall provide the capabilities to prevent unauthorized activities and unauthorized conditions within PA's, VA's, and MAA's. The licensee must provide activity and condition control systems that are able to detect unauthorized activities and unauthorized conditions in sufficient time to permit an effective and acceptable response which prevents unauthorized activities and unauthorized conditions to exist or continue.

The following functions are required of the safeguard system to assure the detection capability. (See Section ___ for required functions of the response capability.)

A. To detect unauthorized activities or unauthorized conditions within PA's, VA's, and MAA's, the following are needed:

1. Authorization Controls: The licensee shall provide authorization controls and procedures that will establish the activities and conditions permitted within each of the areas with unique requirements.
2. Boundaries: The licensee shall define boundaries for the areas that have unique requirements for authorized activities and conditions.
3. Activity and Condition Detection Systems: The licensee shall provide detection systems and procedures that, in a timely manner, will:
 - a.) surveil, monitor and/or inspect each of the defined areas to discover activities and conditions that are not authorized;
 - b.) collect sufficient information for assessment of the nature of the activity and/or condition;
 - c.) assess the information; and
 - d.) appropriately communicate with reaction/response forces.

review
the be
conf

The safeguard system shall provide the capabilities to prevent unauthorized and unconfirmed removal of SNM from MAA's. The licensee must provide removal control systems that are able to detect unauthorized attempts to remove SNM in sufficient time to permit a response, confirm that SNM is being removed in an authorized manner, and provide an effective and acceptable response which prevents unauthorized and unconfirmed removal of SNM.

The following safeguard subsystems are necessary to assure the detection and confirmation capabilities. (See Section ___ for necessary aspects of the response capability.)

A. To detect attempts at unauthorized removal of SNM by stealth from MAA's, the following are needed:

1. Removal Detection Systems: The licensee shall provide detection systems and procedures that, in a timely manner, will:

- a.) detect and annunciate to the reaction and/or response forces any attempts to remove SNM;
- b.) collect sufficient information for assessment of removal attempt characteristics;
- c.) assess the information; and
- d.) appropriately communicate with reaction and response forces.

com
Dr
10/27/73

2. Barriers: The licensee shall provide barriers that will:

- a.) channel exit attempts to exit controls;
- b.) delay any attempts to remove SNM sufficiently to permit the detection and response systems to function in an effective manner.

B. To detect attempts at unauthorized removal of SNM by deceit from MAA's, the following are needed:

1. Removal Authorization Controls: The licensee shall provide authorization controls and procedures that will establish accurate properties for authorized removal of SNM by specifying the characteristics of the SNM authorized for removal, the person(s) authorized to remove the SNM, and the removal schedule.

2. Removal Controls: The licensee shall provide removal controls and procedures that will:

a.) determine the apparent characteristics of the SNM presented for removal;

b.) verify the identity of the person(s) presenting the SNM for removal;

c.) verify the removal schedule;

d.) assess the apparent SNM characteristics and the verified identity and removal schedule against the authorized removal properties; and

e.) appropriately interface with the SNM Confirmation Controls and/or reaction forces.

C. To confirm the identity of SNM presented for authorized removal from MAA's, the following is needed:

1. SNM Confirmation Controls: The licensee shall confirm the authorized removal of SNM by providing controls and procedures that will:

a.) verify the apparent characteristics of the SNM presented for removal;

b.) assess the confirmed SNM characteristics against the authorized characteristics; and

c.) appropriately interface with the reaction force.

- (2) A system, including search of personnel, vehicles, packages and material exiting a material access area, to prevent unauthorized removal of SNM.
- (3) Special containment of high quality, divertible size SNM including isolation of work areas, limited access, surveillance of employees and restrictions on personal articles and clothing (this includes a prohibition against the wearing of metal bearing clothing and the carrying of metal objects thru the material access area exit point).

Accompanying Guides

- Access controls
- Search Techniques and Equipment

F. Testing

- (1) A system, including frequent functional tests, to insure that security equipment sub-systems are operating properly.
- (2) A system to insure that the performance of security organization personnel is adequate.
- (3) A procedure for the integrated testings of the overall facility safeguards system.
- (4) A plan for testing the LLEA response capabilities.

Accompanying Guides

- Alarm System and Communications Testing
- Performance Testing of Security Personnel
- Safeguards System Testing
- Verification of LLEA Response

Handwritten notes:
 - "divertible size" circled
 - "limited access" circled
 - "against the wearing of metal bearing clothing and the carrying of metal objects thru the material access area exit point" circled
 - "for me" written vertically
 - "test" written vertically
 - "in reg" written vertically
 - "with min 10" written vertically
 - "reg free" written vertically
 - "nt es" written vertically

2/2/77

Chapell for Haller - telecom comments on 1/26/77

- threat should be reworked

b ii + iii - omit protected area
b i - iii should be reordered?

- repetitive probs.

3 ii - ~~add~~ add PA to make consistent

4 ii - should be from all locations - not just auth'd.

pg. 5 ~~(c)~~ (c) - QA write-up bad

(d) pg 6 - use com. mode & single failure rather than subsystem & compon. redundancy

ISI BC Narrative

pg. 4 (2) (b) how get adversary "intent"?

(d) - tough to do

- informed Chapell of Chapman comments to WG 2/1/77

SAFEGUARDS UPGRADE RULE STRUCTURE

(Comments from
C. South, TSG
31 Jan 77)

§ 73.50 Requirements for Physical Protection of Licensed Activities
and Special Nuclear Material

In addition to any requirements of this part, each licensee who is authorized to operate a fuel reprocessing plant pursuant to Part 50 of this chapter or who possesses or uses uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium alone or in any combination in a quantity of 5,000 grams or more computed by the formula, $grams = (grams\ contained\ U-235) + 2.5 (grams\ U-233 + grams\ plutonium)$, including licensees who are authorized to operate a nuclear reactor pursuant to Part 50 of this chapter who possess or store such material shall comply with the following requirements. The requirements of this section do not apply to such reactor licensees who possess such material only when it is located in the core of a nuclear reactor and/or who possess or store such material only when it is contained in irradiated fuel elements removed from the reactor core.

(a) General Performance Requirements.

(1) The licensee shall use the following design basis events to establish and maintain an onsite physical protection system and security organization which will provide protection with high assurance against successful theft of special nuclear material or industrial sabotage by both of the following:

(needs to be defined and included)

(i) A determined violent external assault, or attack by stealth of up to persons with the following attributes, assistance and equipment: (A) Well-trained (including military

training and skills) and dedicated individuals, (B) Inside assistance of knowledgeable individual who may attempt to participate in both a passive role (e.g., provide information) and an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), (C) Suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long range accuracy, (D) Hand-carried equipment, including explosives for use as tools of entry or otherwise destroying the facility security system integrity, and

(ii) An internal threat of insider or employee (in any position)

(b) Performance Capabilities and Criteria

In meeting the general performance requirements of paragraph (a) of this section, the onsite physical protection system and security organization shall include but not necessarily be limited to basic capabilities that will assure:

(1) Admission of only authorized personnel and materials into material access and vital areas including:

one or the other, but not both!

③ (i) Barriers designed to assure prevention or delay of penetration until appropriate response can be made,

① (ii) Measures to assure that only authorized vehicles, personnel, and materials are permitted access to ~~protected areas~~, material access areas, and vital areas; and

② (iii) Measures to assure detection of penetration or attempted penetration of ~~protected areas~~, material access areas or

vital areas in sufficient time to permit appropriate response;

(2) Timely detection and effective response to unauthorized conditions of access to special nuclear material or unauthorized activities within material access areas or vital areas including

(i) Measures to assure that special nuclear material is used, processed, and handled only by authorized personnel in an authorized manner;

(ii) Measures to assure that only those personnel whose immediate job function requires access to material access areas or vital areas can gain such access; and

(iii) Measures to assure detection of unauthorized activity or presence in a protected area, material access area or vital area in sufficient time to permit an appropriate response;

(3) Removal of only authorized and confirmed materials from material access areas including:

(i) Material access areas within barriers designed to assure against unauthorized removal of material and to assure control of ingress to and egress from such areas;

(ii) Measures to assure that special nuclear material is not removable or removed from authorized areas except by authorized, controlled routes, at authorized times, in authorized quantities, and by authorized personnel;

(iii) Measures to assure that special nuclear material is used, processed, handled, and stored only in authorized

*one or the other,
but not both!*

areas for authorized purposes;

(4) Timely detection and effective response to breaches in the containment of special nuclear material including:

(i) Measures to assure the detection of unauthorized routes by which special nuclear material could be removed from authorized locations in sufficient time to assure that such routes are not used for unauthorized removals;

(ii) Measures to assure the detection of unauthorized removal or attempted unauthorized removal of special nuclear material from authorized locations in sufficient time to permit a response that will prevent removal of the special nuclear material from the protected area; and

(iii) Measures to assure that emergency conditions cannot be used to compromise material containment systems to effect theft of the material; and

(5) Timely detection and effective engagement of intruders penetrating the protected area including:

(i) Barriers designed to assure prevention or delay of penetration until appropriate response can be made;

(ii) Measures to assure detection of penetration or attempted penetration of the protected area in sufficient time to permit a response that will permit effective engagement of the intruders;

(iii) A security organization composed of personnel trained and ^{equipped} ~~qualified~~ to provide immediate and effective response to penetrations of the protected area;

NOTE: Training is a condition of authorization, as is protection, health, etc.

one or the other, but not both!

- (iv) Preplanned response measures to assure effective response to penetrations^{or attempted penetrations} of the protected area; and
- (v) Communications measures designed to provide for summoning of^{external} aid, if necessary, in response to a threat and for coordination of actions of response forces in counteracting a threat.

(c) Quality Assurance.

The applicant or licensee shall demonstrate the establishment and maintenance of a quality assurance program for special nuclear material safeguards systems to assure control over the activities affecting the effectiveness, reliability, and availability of such systems including demonstration that the quality assurance program will be maintained throughout the plant life to assure that any defective safeguards systems, subsystems, or components are promptly detected and corrected. The criteria for quality assurance programs set forth in Appendix B of Part 50 of this chapter, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," provides guidance regarding the essential elements of a quality assurance program.

(d) Redundancy and Diversity.

Safeguards systems shall be designed against common mode and single failures of subsystems or components that would render the system inoperable or ineffective. Subsystem or component diversity provides protection against common mode failure. For

example, an adversary cannot cut off communication with local law enforcement authority by eliminating the telephone service from the plant if there is also radio service. Subsystem or component redundancy provides protection against single failure. For example, an adversary cannot defeat an alarm system by cutting off the power if there is an emergency or back up power source for safeguards equipment.

(e) Specific Requirements

In meeting the general performance requirements of paragraph (a) of this section, and in assuring the basic capabilities of paragraph (b) of this section, the onsite physical protection system and security organization shall include but not necessarily be limited to capabilities to meet the specific requirements of paragraph (f) through (?) of this section. The Commission may authorize an applicant or licensee to provide measures for protection against theft of special nuclear material and industrial sabotage other than those required by this section if the applicant or licensee demonstrates that the overall level of system performance provides protection equivalent to that which would be provided by paragraphs (f) thru (?).

[Thru (?) would include the specific requirements now in §73.50 and §73.60.]

FIRST PERFORMANCE CAPABILITY NARRATIVE

Access Control subsystems shall provide the capabilities to detect and respond to unauthorized attempts to gain access or introduce unauthorized material into MAAs and VAs. The licensee must provide safeguard systems that are able to detect unauthorized attempts to gain access or attempts to introduce unauthorized material in sufficient time to permit an effective response, and must be able to provide response in an effective and acceptable manner to prevent unauthorized personnel entry or introduction of material.

(Note: the following relates to the personnel access controls only, material access controls will follow later.)

The following ^{Safeguards} ~~safeguard~~ subsystems are necessary to assure the above detection capability. To support this capability, the subsystems must perform the functions identified below. (See Section ____ for details of the response.)

A. To detect attempts to gain access by deceit, the following ^{functions must be provided:} ~~subsystems are needed:~~

- (1) Authorization Controls: The licensee shall provide authorization controls that will (a) establish accurate and updated entry lists, based on routine operational requirements and non-routine/emergency requirements; and (b) establish updated entry requirements based

on the immediate facility situation.

(4) Access to vital areas and material access areas shall be limited to individuals who are authorized access to vital equipment or special nuclear material and who require such access to perform their duties. Authorization for such individuals shall be provided by the issuance of specially coded numbered badges indicating vital areas and material access areas to which access is authorized. 2.50.6.4

(5) Admittance to a material access area shall be ~~under the control of authorized individuals~~ and limited to individuals who require such access to perform their duties. 2.50.6.5

- (2) Entry Controls: The licensee shall provide entry controls to confirm the identity of persons presenting themselves for access, to assess the identity against the authorization and requirements lists, and to appropriately interface with reaction forces.

(c) Access requirements. The licensee shall control all points of personnel and vehicle access into ~~a protected area including shipping or receiving areas and into each vital area~~. Identification of personnel and vehicles shall be made and authorization shall be checked at such point. 2.50.6.5

(5) Admittance to a material access area shall be under the control of authorized individuals. 2.50.6.5

B. To detect attempts to gain access by stealth, the following *functions must be provided:*
~~subsystems are needed:~~

- (1) Barriers: The licensee shall provide barriers that will: (a) channel casual penetration attempts of unauthorized persons to MAA and VA entry controls; and (b) delay penetration attempts by unauthorized individuals sufficiently to permit the detection and response systems to function in an effective manner.

(b) *Physical barriers.* (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. More than one vital area may be within a single protected area.

(2) The licensee shall locate material access areas only within protected areas such that access to the material access area requires passage through at least two physical barriers. More than one material access area may be within a single protected area.

(3) The physical barrier at the perimeter of the protected area shall be separated from any other barrier designated as a physical barrier within the protected area, and the intervening space monitored or periodically checked to detect the presence of persons or vehicles so that the facility security organization can respond to suspicious activity or to the breaching of any physical barrier.

2.5.6.1,2,3

- (2) Detection Systems: The licensee shall provide effective detection systems and procedures that will: (a) detect and annunciate in a timely manner to the reaction and response personnel unauthorized access or penetration attempts of MAAs or VAs; (b) permit the accurate and timely collection of sufficient information for assessment of adversary characteristics and intent; (c) provide for assessment of information and the resulting decisions regarding response force notification in a timely and efficient manner; and (d) permit communications with reaction and response forces in a timely manner.

Detection aid requirement. Each unoccupied material access area shall be locked. Unoccupied vital areas and material access areas shall be protected by an active intrusion alarm system, and

all emergency exits shall be continuously alarmed.

23.50.c.4
23.60.c.