



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

I 26

FEB 13 1977

MEMORANDUM FOR: Llewellyn Evans, Jr., Chief
Security Programs Branch
Division of Safeguards, NMSS

FROM: Ralph J. Jones, Chief
Materials Protection Standards Branch
Office of Standards Development

SUBJECT: REVIEW OF DRAFT CAPABILITY NARRATIVES AND MINIMUM
ESSENTIAL REQUIREMENTS

We have reviewed the subject information submitted with your memo of February 10, 1977, and have the following general comments:

1. The basic capability narratives appear to be complete if one assumes coverage in the two basic capabilities not presented. For example none of the first three capability narratives address violent attack. We assume this will be covered in the narratives for capability 5.
2. The capability narratives are presented logically and it appears that given the complete set of five they would present a logical statement of the performance expected of a licensee's system.
3. The narrative seems to present the logic of each capability and tell what is meant. The language will need to be edited some to assure a clear statement of requirements. For example, the phrase used quite often, "the following are needed" may not make it clear that whatever follows is a requirement of the regulation. The basis is present however and we can work with Mr. Fonner in developing final language.
4. We do not agree with the Minimum Essential Requirements present in the February 4, 1977 draft. Is it mandatory that the licensee use penetration resistant vaults if he has an alarmed vault and sufficiently rapid response to prevent removal of the material? In any case, "penetration-resistant" would need to be defined. It probably would be defined in terms of the response time capability provided. We do not agree that area denial systems such as non-

lethal debilitating vapors or liquids are minimum essential requirements. The legal implication of such measures may preclude their use. Is it essential that there be a "facility-wide" tamper-indicating alarm system linked with LLEA? In some jurisdictions this may not be possible or permitted.

5. The Minimum Essential Requirements were not logically presented in that many of them were restatements of performance requirements and not specification requirements. For example, items A(1), B(1), C(1), and possibly E(1). It seems we need a clearer definition of what is a performance requirement and what is a system specification. We suggest that the term used be "Basic Essential Elements" of a safeguards system rather than using the word minimum. We suggest these basic essential elements are:

- (a) Security organization
- (b) Physical barrier systems
- (c) Access control systems and procedures
- (d) Detection and alarm systems
- (e) Communications systems
- (f) Quality assurance programs for installation, construction, operation, and maintenance of security systems and procedures
- (g) Contingency and response plans and procedures

Within each of these elements then basic essential components and subsystems might be specified. For example, in (a) specific requirements for training, equipping, and qualifying guards might be specified. At present this is done by Regulatory Guide but we are now working on specific requirements and criteria. Under (b) double barriers as now specified in the regulations might be called for or to upgrade we might decide to require double fences for the protected area. Under (g) we are now working on regulatory guides for contingency plans but a rule is presently on its way to the Commission specifying required criteria for contingency plans. We need to look at the basic essential elements and decide what are the essentials that we must require within those elements. We also need to agree on the basic essential elements. The essentials within the elements will be more difficult. It is there that we materially affect the licensees flexibility in designing his system. To assist in this development we enclose a draft Basic Essential Elements list with what we believe are basic essential components and subsystems. We believe the Basic Essential Element list is complete and correct. The essential components and subsystems are more in the context of suggestions.

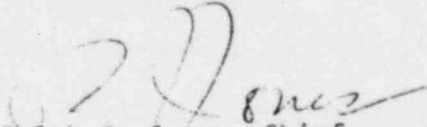
FEB 1 1977

Llewellyn Evans, Jr.

-3-

A major problem will be tying the basic essentials to the basic capabilities. As we see it they cannot be integrated in the regulations without causing some redundancy and confusion. In a separate statement of the basic essentials we could identify for each essential component or subsystem the capability or capabilities to which it applied. For example, barriers are called for in both capability 1 and 3 and presumably also in 5. In the essential requirements section we could identify protected area barriers (double fences perhaps) with capability 1 and 5. (We believe protected area barriers and detection are essential for effective and timely response to prevent unauthorized persons or materials from being able even to reach the MAA or VA boundary or barrier, i.e., a part of capability 1.)

Further, the plant system of authorizations and entry and exit controls would include elements applicable to capability 1 for access to MAAs and VAs as well as the PA, to capability 2 to identify the activities to be conducted in an area as well as the persons conducting them, to capability 3 to identify persons authorized to remove SNM or to authorize its removal and probably to capability 5 for control of persons entering the PA. It would be confusing and redundant to fragment the essential subsystem and component requirements under each of the capability requirements. We believe a separate essential requirements section would be more easily understood and would present a more logical pattern of requirements.


Ralph J. Jones, Chief
Materials Protection Standards Branch
Office of Standards Development

Enclosure:
Draft Basic Essential Elements List

Basic Essential Elements
of
A Safeguards System

A. Security Organization

1. Trained, qualified equipped guard and escort force
2. Written procedures, responsibilities, authorities

B. Physical Barrier Systems

1. Protected areas, vital areas, material access areas
2. Double carrier concept
3. Double perimeter barriers
4. Isolation zones
5. Illumination
6. Enclosed Handling and Process Areas
 - a. locked when unoccupied
7. Storage vaults or vault type rooms
 - a. locked
8. Secure cargo vehicles and containers
9. Armored escort vehicles

C. Access Control Systems and Procedures

1. Authorization procedures
 - a. personnel
 - b. vehicles
 - c. materials
2. Identification and admittance procedures and systems
 - a. personnel
 - b. vehicles
 - c. materials

3. Search procedures and systems

- a. personnel
- b. packages
- c. materials
- d. vehicles
- e. entrances
- f. exit from MAA

4. Control points

- a. hardened

5. Shipment routing and times

- a. minimum times
- b. transfer limits
- c. receiver notices
- d. safe routes

D. Detection and Alarm Systems

1. Perimeter intrusion alarms

2. Interior intrusion alarms

- a. penetration alarms
- b. space alarms

3. Area surveillance systems and procedures

- a. CCTV
- b. patrols
- c. buddy system
- d. transfer point surveillance

4. Dual alarm stations
 - a. manned
 - b. hardened
 - c. alarm location indication

5. Duress alarms

6. Fail-safe and Tamper-indicating

E. Communication Systems

1. On-site guards and control centers

- a. fail-safe procedures
- b. continuous

2. On-site tactical system

3. Off-site to LLEA or other assistance forces

- a. dual systems
- b. fail-safe procedures
- c. continuous

4. Within convoy

5. Convoy to base

- a. continuous
- b. fail-safe procedures

F. Quality Assurance Program

1. Tests and inspections

- a. design
- b. installation and construction
- c. preoperational
- d. operational

2. Preventive maintenance
3. Corrective action procedures
4. Records and reports
5. Audits

G. Contingency and Response Plans and Procedures

1. Liaison with LLEA
2. Threat assessment procedures
3. Action plans and procedures
4. Responsibility matrix

U.S. FEDERAL REGULATORY COMMISSION
ROUTING SLIP

Organization	
NAME - MAIL STOP	
Charles South	→
Bud Evans	f-10
Tom Tluyer wanted T. Carter's branch represented in the review cycle and T. Long was named. His comments are furnished for possible use.	
C. South	

REMARKS:
Marked on attached copy are comments on the "Upgrade Rule Activity" transmitted by Bud Evans on 10 February.

- | | | |
|---|--|---|
| <input checked="" type="checkbox"/> Requested | <input type="checkbox"/> See Me | <input type="checkbox"/> Note and Return |
| <input type="checkbox"/> Correction | <input type="checkbox"/> Approval/Signature | <input type="checkbox"/> Per Conversation |
| <input type="checkbox"/> File | <input type="checkbox"/> Comment/Concurrence | <input type="checkbox"/> Answer/Acknowledge for |
| <input type="checkbox"/> Information | <input type="checkbox"/> Necessary Action | Signature of _____ |

FROM (Name) *J. Long* OFFICE SGCP DATE 14 Feb 77
PHONE 2-7231

Basic Capability 1 Narrative

include?
stealth or by direct
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

How many "systems" are there? (could it just be including the sub-systems?)

Handwritten notes and scribbles on the left margin.

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 ^{maintain} updated entry requirements;
 - b.) establish ^{and maintain open} 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.

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.

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.

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 unauthorized 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.
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 actual} ~~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 ^{actual} ~~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 ^{be able to} ~~confirm~~ the ~~an~~ authorized removal of SNM by providing controls and procedures that will:
 - a.) verify the ^{actual} ~~apparent~~ characteristics of the SNM presented for removal;

revised: see (a)

- b.) assess the confirmed SNM characteristics against the author characteristics; and
- c.) appropriately interface with the reaction force.

J. J. Kasun
2/4/77

SAFEGUARDS UPGRADE RULE

Minimum Essential Requirements

A. Security Organization

*How! The
interview was
repet.*

- (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

Barrier Design

- (1) A system of barriers to delay or deny entrance by personnel and vehicles into the protected area, vital areas and material access areas.
- (2) Penetration 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

*potential
in losses*

C. Communications

- (1) Capability for continuous radio voice communication between the guard force and alarm and control stations and between the facility and LLEA.
- (2) A facility-wide tamper-indicating duress alarm system linked to LLEA.

Accompanying Guides

- Duress alarm system

D. Intrusion Alarm System

- (1) An electronic 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 assessment of (i) a perimeter or interior alarm and (ii) the nature and extent of a threat (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.

*is this
function?*

- (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

COMMENTS ON THE UPGRADE RULE THIRD OPTION DRAFT
MATERIAL INCLUDED WITH THE FEB. 10, 1977 STATUS RPT.

GENERAL - There appears to be a mismatch between the intent stated in the status report memorandum and the attachments, particularly the "Minimum Essential Requirements" attachment. Specifically, the first paragraph of the memo states the third option to integrate both performance requirements and minimum essential system specifications. Clearly, the named attachment is not a system specification statement, minimum or otherwise. It is not even a statement of minimum requirements as the title implies, since many imprecise descriptive words are used such as: delay, resistant, high assurance, rapid, high quality, frequent, properly, etc. Definitions for each of these will have to be generated if they are retained, otherwise restatements are necessary.

Whether or not the attachment could ever achieve status as a specification would depend on the specificity NRC is prepared to offer for each of the items. Sections A, Security Organization, and E, Control of Entry and Exist, are better in this regard than the other four, with the poorest being section D, Intrusion Alarm System. Close behind is the section on testing, section F. One last thought on this attachment; the words "minimum essential" are unnecessarily redundant. Either alone is sufficient.

With regard to the other attachments on the basic capability narratives, the structure appears to be correct and complete, although

changes are required in some areas to clarify the intent or avoid redundancy. For this purpose, specific comments are offered on a marked up copy attached to these comments. This includes the other attachment as well.

CONCLUSION - Per the request to group comments on the documents in three categories, the following is offered in the order specified. (1) With the corrections included per the marked up copy, the three basic capability narratives would be improved and correct, but not complete until the intended integration is accomplished. The other attachment requires considerable work. (2) Yes, the sections are organized logically. (3) Only the author(s) can say what the narrative was meant to say. What appears in the attachments, as amended per comments, would say what should be said at this point in the rule making cycle.

A last overall comment is warranted on this option concerning its viability as a candidate worth pursuing further. I think not. There is merit in developing and offering option 1, the totally integrated version. There is convenience in pursuing option 2 as stated, if by "detailed systems specifications" is meant the retention and update of applicable CFR's with or without generic based license conditions. The reasons for favoring these are: (a) the first is a form of systems approach to the problem and is long overdue, and

(b) retention of the CFR's in some form should ameliorate the licensee reaction in that he has at least learned to cope with them and would find few surprises.

Option 3, however, is not a systems approach and has none of the appeal of option 1, nor the convenience feature of option 2. We would, in fact, be hard pressed to support and defend option 3 if it were chosen and we had to do so at some future date. It appears to be an idea whose time has not yet come.

C. South