



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

March 4, 1977

MEMORANDUM FOR: L. J. Evans, Jr., Chief
Requirements Analysis Branch
Division of Safeguards, NMSS

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

SUBJECT: FIFTH BASIC CAPABILITY

We have reviewed the narrative for the fifth capability submitted with your memo of March 2, 1977.

Rewording the capability from that used in the Joint Task Force report has caused it to be incomplete. The narrative refers to the five basic functional capabilities, but there are only four in addition to the response capability. By merely providing response to the preceding four capabilities, there is no response to the armed intruder since that type of adversary is not addressed in any of the first four capabilities. We suggest the wording in the Joint Task Force be retained or at least something closer to it so as to include the armed intruder.

The sections do not appear to be completely logical in that there is redundancy and misplaced subfunction statements. For example, liaison with LLEA is listed under Security Organization, Response Plan and Communications. We do not believe this is a part of the Security Organization, but rather a part of the Response Plan. The listing is proper as it is under Communications. Item d, under Communications, appears to be more of a reporting requirement rather than a security function.

The narrative says most of what it should say given a return to the task force language. However, it seems to go into too much detail in the subfunctions. Under Security Organization, items b, c, d, and e are components of the licensee's contingency plan or security procedures plan and do not need to be identified separately in the capability statement.

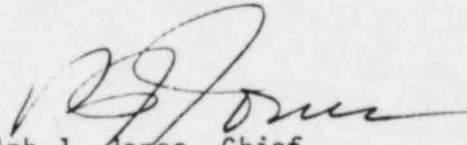
To stay approximately with the Joint Task Force wording, the attached outline is suggested. This tends to leave out response to the other capabilities but they could be added in each case. This might

L.J. Evans, Jr.

- 2 -

be a better approach because the response could be different in each case. On the other hand, it might be simpler to add for the first capability the phrase "or force" to the function to detect attempts at access by stealth, i.e., "detect attempts to gain access by stealth or force" In either case, it seems the subfunctions for the response capability would be the same. Alternate wording is suggested in the enclosure.

Also enclosed is a comparison of basic capabilities to basic essential elements. Input from the task group on this should permit us to write the rule. If we could discuss this in detail at the next meeting, we should be able to have a draft rule by the meeting following that, i.e., about March 16th.



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

Enclosures
As stated

RESPONSE CAPABILITY

The safeguards system shall provide the capability for detection of intruders penetrating the protected area in sufficient time to effectively engage such intruders.

or

The safeguards system shall provide the capability to respond to events detected in the four functional capabilities required in sections _____ in a time and manner sufficient to prevent the theft or diversion of SNM or sabotage of the facility.

The following safeguards functions and subsystems are required to assure the adequacy of this capability:

1. Security Organization: The licensee shall establish a security organization that will:
 - (a) provide trained and qualified personnel to carry out assigned duties and responsibilities, and
 - (b) provide effective routine security operations and planned and effective response to emergencies and safeguards contingencies.
2. Contingency Plans: The licensee shall establish a pre-determined plan of decisions and actions in response to safeguards contingency events that will:
 - (a) provide immediate and rapid assessment of a contingency, and
 - (b) provide predetermined decision alternatives and courses of action by security organization and operations personnel in response to events.
 - (c) provide a matrix of assigned responsibilities for decision and action in contingency situations.
3. Equipment and Facility Design: The licensee shall provide equipment for the security organization and facility design features that will:
 - (a) provide for rapid assessment of safeguards contingencies,
 - (b) provide for rapid and effective response by appropriate security organization personnel, and
 - (c) minimize exposure of assessment and response personnel

4. Communications: The licensee shall provide communications facilities and equipment that will:

- (a) provide rapid and accurate transmission of security information among on-site forces for routine security operation, assessment of a contingency and response to a contingency, and
- (b) provide rapid and accurate transmission of detection and assessment information to off-site assistance forces

Basic Capabilities/Basic Essential Element Comparison

Basic Capability

Essential Element Reference

- | | |
|---|-----------------------|
| I. Assure admission of only authorized personnel and materials into material access and vital areas: | |
| A. Detect attempts to gain access or introduce material into MAA's or VA's by stealth or force: | |
| 1. Access Detection System: | |
| a. detect and alarm | D.1, 2, 3, 4, 5, 6 |
| b. assess alarm | B.3, 4; D.4a, 4c; E.1 |
| 2. Barriers: | |
| a. channel personnel and materials to entry control points | B.1; C.4 |
| b. define area boundaries | B.1. |
| c. delay penetration | B.1, 2, 5, 6 |
| B. Detect attempts to gain access or introduce material into MAA's or VA's by deceit: | |
| 1. Access Authorization Controls: | C.1 |
| a. entry requirements | |
| b. authorization procedures and schedules | |
| 2. Entry Controls: | C.2, 3,4 |
| a. identify persons and materials | |
| b. verify authorizations | |
| C. Communicate attempts by stealth, force, or deceit to provide for response to prevent unauthorized access | D.4c; E.1; G |

II. Assure timely detection and effective response to unauthorized activities and conditions within PA's, VA's, and MAA's:

A. Detection of unauthorized activities or conditions:

1. Boundaries for areas in which only authorized activities and conditions are permitted:

B.1, 5, 6

2. Authorization Controls:

a. establish authorized conditions and activities

C.1

3. Detection System:

a. surveil, monitor, inspect areas

D.3

b. assess activities and conditions

C.3

B. Communicate unauthorized activities or conditions to provide response to prevent theft of material or sabotage

E.1; G

III. Assure removal only of authorized and confirmed materials from MAA's:

A. Detection of attempts at unauthorized removal of SNM by stealth:

1. Detection System:

a. detect and alarm

C.3f; D.2

b. Assess alarm

C.4; D.4

2. Barriers

a. channel exit

B.1; C.4

b. delay removal

B.1, 2, 5, 6

B. Detection of attempts at unauthorized removals by deceit:

1. Removal Authorization Controls

70.51(e)(1); 70.54; 70.58(d) & (h)

- a. removal schedules
- b. material quantity and properties
- c. authorized personnel

2. Removal Controls

- a. identify material quantity and properties
- b. verify removal schedule and material quantity and properties

70.51(e)(1); 70158(d)(e) & (h)

- D. Communicate unauthorized removal attempts to provide response to prevent removal

D.4c; E.1; G

IV. Assure timely detection and effective response to breaches in the containment of SNM:

A. Surveillance and Test Procedures:

- 1. Surveillance and Inspections
- 2. Test Procedures

D.3; F.1, 2, 5
F.1

B. System Analysis:

- 1. Diversion Path Analysis
- 2. Black Hat Modelling

F.1c

- C. Communicate containment breach information for correction before material can be stolen or diverted:

- 1. Corrective action procedures

F.3, 4

V. Assure timely and effective response to contingency events detected in capabilities I through IV:

A. Security Organization:

- 1. Trained and qualified personnel
- 2. Security procedures and planned response actions

A.1, 2
A.3; G

B. Contingency Plans:

G

1. Assessment procedures
2. Predetermined response decisions and actions
3. Responsibility matrix

C. Equipment and Facility Design:

B.3.4; E.1

1. Assessment of contingency
2. Rapid and effective response
 - a. personnel
 - b. equipment
 - c. procedures
 - d. facility design

A.1, 2

A.1

A.3; G

B.2, 5, 6; C.4; D.1, 2, 3, 4, 6

3. Personnel protection

C.4a; D.4b, 4d, 5

D. Communications:

1. On-site security forces and detection systems
2. Off-site assistance forces

E.1

E.2

Ted Sharr

BC - 4 (Containment)

- ① Focus on S/G system as opposed to adversary action
- ② Concerned w/ access to area or mat. (legit. distins)
- ③ purpose is to provide warning & delay
- ④ call unauthor'd movement ^(control)
(under that worry both access + removal)

- "movement" connotes adversary action
 - "control" " " S/G system focus

- ⑤ Should we worry about add'l contain against "good" mat?
 - if yes then asking for higher legit. level of S/G consid. across all BC's