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

March 17, 1977

MEMORANDUM FOR: Upgrade Working Group

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

SUBJECT: BASIC CAPABILITY REGULATORY PROVISIONS AND COMPARISON OF BASIC CAPABILITIES WITH BASIC ESSENTIAL ELEMENTS

Attached please find drafts of:

- A complete set of revised basic capabilities regulatory provisions,
- A basic capability overview writeup,
- Disaggregation of basic capability charts,
- A cross-reference comparison of the basic capabilities with the basic essential elements, and
- A matrix manifesting explicit and implicit basic capability coverage of the basic essential elements.

The matrix, and the comparison of the basic capabilities with the basic essential elements are for your information and need not be commented upon.

The basic capability regulatory provisions and overview writeup are circulated as a complete set, along with the disaggregations, in order to provide you an opportunity to comment on the capabilities as a complete set. As in the past, these comments should be organized to address the following quests:

1. Are all the sections and entries complete?
2. Are the sections organized logically?
3. Are the narratives concise and do they say what you believe should be said?

MEMORANDUM FOR: Upgrade Working Group

March 17, 1977

Please submit any comments that you have by COB Wednesday, March 23rd. We will have a meeting regarding your comments on Friday, March 25th, at 2pm in Room 825, Willste Building.

Bud Evans

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

Attachments

DISTRIBUTION:

Upgrade Working Group

IE: O. Chambers

SD: R. Jones
T. Michaels

ELD: R. Fonner

NRR: J. J. Miller

SGCL: Mike Smith

SGPS: D. Kasun

SGTE: C. South

SGPP: B. Hatter

SGRA: A. Poltorak
B. Nulsen

Information List

SG: R. Page

SGOE: B. Erickson
T. Thayer

SGLI: R. Brightsen

SGPP: E. Perchonok

SGCL: E. McAlpine

SGTE: F. Crane

SGRT: J. Powers

SGTA: T. Sherr

SGRA: D. Sutton
D. Kunihiro

RES: F. Arsenault

IE: D. McCormick
N. Haller

SD: J. Prell
R. Ramirez

NRR: M. Elliott

3/17/77

DRAFT

BASIC CAPABILITY + REGULATORY PROVISION

Capability 1: Admit only authorized persons, material and vehicles into VAs and MAAs.

The licensee safeguards system must include access control systems for VAs and MAAs that are able to detect unauthorized attempts to gain access by persons and detect attempts to introduce unauthorized material and vehicles in sufficient time to permit an effective and acceptable response.

The following safeguards subsystem functions are required to assure this detection capability. (See Section _____ for required functions of the response capability.)

A. To detect attempts to gain access by stealth or force into MAAs and VAs, the following are needed:

1. Barriers: The licensee shall delineate VAs and MAAs with systems that will:

a) channel casual penetration attempts of persons, materials and vehicles to VA or MAA entry controls;

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

2. Access Detection: The licensee shall provide systems and procedures that will:

a.) detect and annunciate to the reaction force any access or penetration attempts of VAs and MAAs by persons and of material or vehicles;

b.) collect and assess information to determine the adversary

c) appropriately communicate with reaction and response forces.

B. To detect attempts to gain access by deceit into MAAs and VAs, the following are needed:

1. Access Authorization: The licensee shall provide systems and procedures for personnel, material and vehicle access that will:

a) establish accurate and updated SNM access authorization requirements for each VA and MAA; and

b) establish updated VA and MAA entry requirements;

2. Entry Controls: The licensee shall provide systems and procedures that will:

a) determine and verify the identity of persons, material and vehicles presented for access;

b) assess the verified identity against the authorization and entry requirements; and

c) appropriately interface with the reaction force.

DRAFT

3/17/77

BASIC CAPABILITY 2 REGULATORY PROVISION

Capability 2: Permit only authorized activities and conditions within PAs, VAs and MAAs.

The licensee safeguards system must include 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.

The following safeguard subsystem functions are required to assure this detection capability. (See Section ____ for required functions of the response capability.)

A. To detect unauthorized activities or unauthorized conditions within PAs, VAs, and MAAs, the following are needed:

1. Boundaries: The licensee shall define locations to be controlled for authorized activities and conditions.

2. Authorization: The licensee shall provide systems and procedures that will establish accurate and updated activities and conditions permitted within each of the defined locations.

3. Activity and Condition Detection: The licensee shall provide systems and procedures that will:

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

b) collect and assess information against the authorizations to determine the impact of the activity and/or condition; and

c) appropriately communicate with reaction and response forces.

DRAFT

3/17/77

BASIC CAPABILITY 3 REGULATORY PROVISION

Capability 3: Permit only authorized location and movement of SNM within MAAs.

The licensee safeguards system must include SNM control systems that are able to detect unauthorized location and movement of SNM within MAAs in sufficient time to permit an effective and acceptable response.

The following safeguards subsystem functions are required to assure this detection capability. (See Section ____ for required functions of the response capability.)

1. Constraints: The licensee shall delineate authorized locations and controls that will:

   a. limit access to and exposure of SNM; and

   b. minimize the movement of SNM.

2. Location and Movement Authorization: The licensee shall provide systems and procedures that will:

   a. establish the authorized location and/or control of all SNM;

   b. establish authorized access to SNM; and

   c. provide for the authorized movement of and operations on SNM within the MAA.

3. Location and Movement Detection: The licensee shall provide systems and procedures that will:

   a. assure discovery of SNM in unauthorized locations and/or not under authorized control;

   b. discern unauthorized access to SNM;

   c. assure discovery of unauthorized movement of SNM;

DRAFT

d. collect and assess information against the authorizations to determine the impact of the detected condition; and

e. appropriately communicate with reaction and response forces.

3/17/77

This section needs a lot of work done on it. It is mostly words w/o substance — not well-organized

DRAFT

BASIC CAPABILITY 4 REGULATORY PROVISION

Capability 4: Remove only authorized and confirmed SNM from MAAs

The licensee safeguards system must include removal control systems that are able to detect unauthorized attempts to remove SNM and confirm that SNM is being removed in an authorized manner, in sufficient time to permit an effective and acceptable response.

The following safeguard subsystem functions are required to assure these detection and confirmation capabilities. (See Section ____ for required functions of the response capability.)

A. To detect attempts to remove SNM by stealth or force from MAAs, the following are needed:

1. Barriers: The licensee shall provide systems that will:

a) channel exit attempts to MAA removal controls;

b) delay any attempt to ~~remove~~ SNM sufficiently to permit the detection and response systems to function in an effective manner.

2. Removal Detection: The licensee shall provide systems and procedures that will:

a) detect and annunciate to the reaction force any attempt to remove SNM;

b) collect and assess information to determine the removal attempt characteristics; and

c) appropriately communicate with reaction and response forces.

Where are search requirements? Should there be some?

Basic Capability 4

B. To detect attempts at removal of SNM by deceit from MAAs, the following are needed:

1. Removal Authorization: The licensee shall provide systems and procedures that will establish accurate requirements 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 properties (e.g., containment, time of removal, mode of transport, etc.).

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

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

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

c) determine and verify the removal properties;

d) assess the apparent SNM characteristics and the verified identity and removal properties against the authorized removal requirements; 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 MAAs, the following is needed:

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

DRAFT

Basic Capability 4

a) confirm 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.

3/17/77

DRAFT

BASIC CAPABILITY 5 REGULATORY PROVISION

Capability 5: Timely detection and effective response to intrusion of PAs.

The licensee safeguards system must include intrusion control systems for PAs that are able to detect unauthorized access or attempts by persons, vehicles and/or materials in sufficient time to permit an effective and acceptable response.

The following safeguards subsystem functions are required to assure this detection capability. (See Section ____ for required functions of the response capability.)

A. To detect attempts to gain access by stealth or force into PAs, the following are required:

1. Barriers: The licensee shall delineate the PA with systems that will:

a) channel casual penetration attempts of persons, material, and vehicles to the entry control;

b) delay penetration attempts of persons and introduction of material and/or vehicles sufficiently to permit the detection and response systems to function in an effective manner;

2. Intrusion Detection: The licensee shall provide systems and procedures that will:

a) detect and annunciate to the reaction force any access or penetration attempts of the PA by persons, and of materials and vehicles;

b) collect and assess information to determine the adversary characteristics; and

c) appropriately communicate with reaction and response forces.

B. To detect attempts to gain access by deceit into PAs, the following are required:

1. Access Authorization: The licensee shall provide systems and procedures for personnel, material and vehicle access that will:

a) establish accurate and updated access authorization requirements for PA entry; and

b) establish updated PA entry requirements.

2. Entry Controls: The licensee shall provide systems and procedures that will:

a) determine and verify the identity of persons, materials and vehicles presented for access;

b) assess the verified identity against the authorization and entry requirements; and

c) appropriately interface with the reaction force.

DRAFT

RESPONSE CAPABILITY

The licensee safeguards system must include a response capability that, in an effective and acceptable manner, will provide the reaction and response functions required by the five basic functional capabilities described in Sections ____. The following functions are required to assure the response 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 established procedures and plans of the safeguards system;

b) provide command and control to reaction and response forces for direction and coordination of activities to assure an effective and acceptable response; and

c) establish liaison with LLEA and other organizations to assure their assistance to reaction forces in case of emergency.

2. Response Procedures and Plans: The licensee shall establish procedures and plans that will:

a) assure effective routine security operations;

b) provide assessment methods for evaluation of detected situations based on established authorization;

c) provide predetermined decision alternatives and courses of action for security organization and operations personnel in response to events (ref. Contingency Plan, Appendix B); and

d) provide for implementing LLEA and/or other security organization assistance.

3. Equipment and Facility Design: The licensee shall provide equipment for the security organization and incorporate facility design measures that will:

a) assist the performance of the assessment and response activities;

b) facilitate the implementation of assessment and response activities (provide primary and secondary alarm stations to facilitate assessment and command, control and communication activities);

c) limit exposure of reaction/response force personnel while interfacing with adversaries; and

d) limit opportunity for access to SNM.

4. Communications: The licensee shall provide communication equipment and facilities to:

a) interface with the detection capability to permit rapid and accurate transmission of security information to the reaction and/or response forces;

b) notify LLEA of need for assistance, as identified in the response plan;

c) coordinate reaction and response forces; and

d) alert appropriate authorities (key personnel/appropriate agencies) of non-routine situations as identified in the response plan.

3/17/77 -

DRAFT

BASIC CAPABILITY R ATORY PROVISIONS OVERVIEW

The basic performance capability regulatory provisions, attached, were designed to establish a regulatory base for the upgraded physical protection of SNM against theft and diversion at fuel cycle facilities. Although not specifically designed to assure upgraded coverage against sabotage, these capabilities also provide for increased protection against this adversary goal. In addition, it should be noted that provision has been made for interfacing between these capabilities and future material accounting upgrade recommendations (see Basic Capability 3).

Stated simply, the basic performance capabilities are:

- Admit only authorized personnel, material, and vehicles into MAAs and VAs;
- Permit only authorized activities and conditions within PAs, VAs, and MAAs;
- Permit only authorized location and movement of SNM within MAAs;
- Remove only authorized and confirmed SNM from MAAs;
- Assure timely detection and effective response to intrusion of PAs;

In order to assure complete coverage of all potential strategies for theft and diversion of SNM, the basic performance capabilities were designed to provide diverse interruptions of generic action sequences necessary for achieving those goals. This can be illustrated with the following chart

which manifests the focus, scope, and location of the basic performance capabilities.

	Focus (1)	Scope (2)	Location
BC 1	Access	Pers., mats., vehicles	MAA, VA Boundary
BC 2	Persons & things	Activities & conditions	Within PA, MAA, VA
BC 3	SNM	Location & movement	Within MAA
BC 4	Removal	SNM	MAA Boundary
BC 5	Intrusion	Pers., mats., vehicles	PA

(1) Focus - topic to which primary attention is directed

(2) Scope - characteristics which delineate the applicability of the focus

Thus the capabilities provide for interrupting an adversary upon his:

- intruding the PA
- entering the MAA
- undertaking unauthorized activities within the MAA (or VA and PA)
- moving SNM within the MAA
- removing SNM from the MAA

The approach taken to assure implementation of an appropriate safeguard system was to develop a hierarchy of functions required to achieve each basic capability. Associated with each function is a level of performance describing the degree to which the safeguard system must implement the respective function. This functional hierarchy is developed until a measurable level of performance is reached or until site specific factors influence the prescribed level.

For example, the functions required for the basic capability to allow only authorized access into MAAs and VAs are detection of all access attempts and response to unauthorized access. The subfunctions required to implement detection of access by deceit are:

- Establishing access authorization requirements
- Establishing entry requirements
- Determining and verifying access identity
- Assessing identity vs the requirements
- Interfacing with reaction force

and for detection of access by stealth and force,

- Channeling entry
- Delaying penetration
- Detecting access attempts
- Collecting and assessing information
- Communicating with reaction force

The levels of performance associated with the subfunctions reflect site specific factors, thus the hierarchy is stopped.

Overlaid on this structure of functions and performance levels is a structure of systems of various complexity necessary to implement the functions. These systems become site specific in detail at the same time as the level of performance, thus stopping the hierarchy at the same level of detail.

For example, an access control system is needed to achieve the first basic capability, and implements the detection and response functions. The subsystems needed to implement the subfunctions are barriers, detection systems, access authorization controls, and entry controls. Any further detail, like types of barriers, becomes site specific.

Thus, the attached basic capability regulatory provisions are designed to require all of the generic functions and performance levels, and systems and subsystems without which a facility safeguard program could not satisfy the stated capability. Taken as a set, the capabilities are also designed to assure complete coverage of all strategies (at specified adversary levels) for the theft or diversion of SNM at fuel cycle facilities.

Upgrade Working Group

March 14, 1977

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) 878
B. Erickson (SG)
J. Powers (SG)
T. Thayer (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)
D. McCormick (IE)