



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

March 8, 1977

MEMORANDUM FOR: Upgrade Working Group

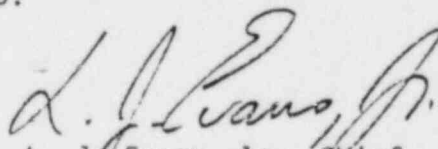
FROM: L. J. Evans, Jr., Chief
Requirements Analysis Branch

SUBJECT: DRAFT OF 5th CAPABILITY NARRATIVE

Attached please find the draft of the 5th capability narrative. With the circulation of this capability at least one draft of all of the capabilities have now been distributed for working group review.

As you have done with other capability narrative documents, it would be helpful if you would organize your comments under the following categories: (1) Are all sections and entries complete? (2) Are all sections organized logically? and (3) Is the narrative concise and does it say what you believe should be said? Please submit your comments on the attached draft by c.o.b. Monday, March 14, 1977.

We will have a meeting on Wednesday, March 16, at 2 p.m. in Room 825 Willste Building to review the comments received regarding this capability and to discuss the organization and overall coverage of the revised capabilities in toto.


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

Attachment

8212080101 821025
PDR FOIA
WEISS82-441 PDR

ENCLOSURE
March 8, 1972

BASIC CAPABILITY 5 NARRATIVE

Is there a separate one for reaction to unauthorized access?

Capability 5: Protect against unauthorized access to protected areas.

The licensee safeguards system must include penetration control systems which protect against unauthorized access to PAs by persons, vehicles and/or materials, by providing for the capability to detect such access or attempts in sufficient time to permit an effective and acceptable response.

The following functions are required to assure this detection capability. (See Section _ for necessary aspects of the response capability.)

A. To detect attempts to gain access by deceit across PA boundaries, the following are required:

1. Authorization: The licensee shall provide systems and procedures that will:

a) establish accurate authorization entrance rosters for personnel, material, and/or vehicle PA entry; and

b) establish updated PA entry requirements for personnel, material and vehicles.

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

a) determine and verify the identity of persons presenting themselves for access and/or materials and vehicles presented for introduction;

b) assess the determined and verified identity, material and/or vehicle against the authorization and entry requirements, and

c) appropriately interface with the reaction forces.

what about...

What about protected positions for security force...

*What about protected positions for security force
of vehicles admitting personnel?
Search to prevent unauthorized access?*

B. To detect attempts to gain access by stealth or force across PA boundaries, the following are required:

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

- a) define the PA area and channel casual penetration of persons, material, and vehicles to the entry control function;
- b) delay penetration attempts of persons and introduction of material and/or vehicles sufficiently to permit the detection and response capabilities to function in an effective manner;

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

- a) detect and annunciate to the reaction force any PA access or penetration attempts by persons, and of materials and vehicles;
- b) collect sufficient information for assessment of the penetration characteristics and extent;
- c) assess the information; and
- d) appropriately communciate with reaction and response forces.

What about timing? - at time of penetration?

remotely? Can we do less - then called for in 73.55?

are we missing the thing to emphasize?

What about lighting around plant perimeter and within PA?

What about control of people outside of perimeter within PA's?

I 9
Thayer

Upgrade Working Group

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)
- 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)
- M. Levy (SG)
- J. Prell (SD)
- R. Ramirez (SD)

To Bud Evans
 My comments
 are in text,
 Tom Thayer
 3/10/77



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

March 8, 1977

MEMORANDUM FOR: Upgrade Working Group

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

SUBJECT: DRAFT OF 5th CAPABILITY NARRATIVE

Attached please find the draft of the 5th capability narrative. With the circulation of this capability at least one draft of all of the capabilities have now been distributed for working group review.

As you have done with other capability narrative documents, it would be helpful if you would organize your comments under the following categories: (1) Are all sections and entries complete? (2) Are all sections organized logically? and (3) Is the narrative concise and does it say what you believe should be said? Please submit your comments on the attached draft by c.o.b. Monday, March 14, 1977.

We will have a meeting on Wednesday, March 16, at 2 p.m. in Room 825 Willste Building to review the comments received regarding this capability and to discuss the organization and overall coverage of the revised capabilities in toto.

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

Attachment

Date of 8212080101

BASIC CAPABILITY 5 NARRATIVE

Capability 5: Protect against unauthorized access to protected areas.

The licensee safeguards system must include penetration control systems which ~~protect~~ ^{prevent} against unauthorized access to PA's by persons, vehicles and ~~the~~ materials, by ~~providing for the capability to detect~~ ^{ing} such access or attempts in ~~sufficient time~~ ^{quickly enough} to permit an effective and acceptable response.

The following functions are required to assure this detection capability. (See Section _ for necessary aspects of the response capability.)

A. To detect attempts to gain access by deceit across PA boundaries, the following are required:

1. Authorization: The licensee shall provide systems and procedures that will ~~maintain~~ ^{and maintain} ~~accurate, authorization entrance registers for~~ ^{up-to-date registers to authorize entry of} personnel, material, and ~~for~~ vehicle ~~PA~~ ^{entry}; and

^{What does this mean?} b) establish updated PA entry requirements for personnel, material and vehicles.

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

? a) determine and verify the identity ^{and authorization} of persons presenting themselves for access, and/or materials and vehicles ~~presented for introduction,~~

b) assess the determined and verified identity, material and/or vehicle against the authorization and entry requirements, and

? c) appropriately interface with the reaction forces.

what does this mean?

B. To detect attempts to gain access by stealth or force across PA boundaries, the following are required:

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

a) define the PA area and channel casual penetration of persons, material, and vehicles to the entry control function;

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

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

a) detect and annunciate to the reaction force any PA access or penetration attempts by persons, ~~and of materials and vehicles;~~ ^{unauthorized?} ~~or~~

b) collect sufficient information for assessment of the penetration characteristics and extent;

c) assess the information; and

d) appropriately communicate with reaction and response forces.

*penetrate
means to
get in!
about it!*

*This is short,
why use PA instead of protected area?*

I 10

*of Applied Comments
Trans.*

ROUTING AND TRANSMITTAL SLIP		ACTION	
1 TO (Name, office symbol or location) BUD EVANS,	INITIALS	CIRCULATE	
	DATE	COORDINATION	
2	INITIALS	FILE	
	DATE	INFORMATION	
3	INITIALS	NOTE AND RETURN	
	DATE	PER CONVERSATION	
4	INITIALS	SEE ME	
	DATE	SIGNATURE	
REMARKS			
<p>Attached are comments on the "Basic capabilities needed to protect SNM while in-transit". They are in the form of annotations to the draft document. General comment — the scope and approach have not been given enough thought - yet!</p> <p><small>Do NOT use this form as a RECORD of approvals, concurrences, disapproval, clearances, and similar actions</small></p>			
FROM (Name, office symbol or location)		DATE	
OS Chambers		3/9/77	
		PHONE	53214/5

DRAFT

MARCH 1, 1977

BASIC CAPABILITIES, NEED TO PROTECT
SNM WHILE IN-TRANSIT

V

SCOPE

The purpose of this paper is to set forth a list of generalized basic capabilities that are necessary for a transportation company to perform to protect SNM against theft or diversion during the SNM in-transit phase of the nuclear fuel cycle. Before the basic capabilities are discussed, it would be helpful to state the scope and to define the terms used in this paper. In addition it would be useful to mention some of the transportation characteristics which lead to the uniqueness of in-transit security requirements.

The term transport is used in a generic sense to denote any land, sea or air conveyance. Thus transport covers such common carriers as trucks, ships, airplanes and rail cars. Although much of the discussion and the basic capabilities are written with particular emphasis on truck transportation, the generalities should apply equally to other modes. When the commonality is difficult to discern, the variances between the modes will be delineated.

There are certain transport operational characteristics that must be considered before capabilities can be established. The more obvious features are the transport mobility and vulnerability; and the phasing of transportation operations. The mobility of a transport gives it the advantage of being able to avoid a dangerous situation and the disadvantage of having to plan for protection over a wide variety of geographical locations and situations. Transports are especially vulnerable to take-overs by hi-jacking techniques. This gives the adversary an added advantage of designing an operation to gain control of the transport first

*How much
by making trucks
power many
of change size
of each ship*

wing

OK!

at a time and location of his choosing

and then removing the SNM at his convenience. The operational phasing of SNM shipments into movement and transfer point operations, confronts the shippers with a wide variety of planning contingencies. Transports within protected areas, at fixed site transfer-points, are perhaps the least complex to protect because the fixed site security force is available to augment the drivers and guards. Transfer points at seaports, airfields and rail heads are not usually within protected areas as defined by CFR 73.2 g; and thus are sufficiently different in character that special planning precautions have to be taken to assure adequate protection.

A final point is that the complexity of protecting SNM while in-transit, from a covert attempt to steal it, is different and perhaps less demanding than protecting SNM at a fuel cycle facility; since the material aboard a transport, is never exposed or handled during the in-transit phase. This, of course, means that there is no requirement to inspect for diverted material among the drivers and guards while enroute in the same manner that a fuel cycle facility inspects for SNM among the employees before entering and leaving MAAs and VAs. Once the SNM is loaded and sealed on the transport, no one is authorized to open the sealed container until the shipment reaches its ultimate destination.

VERY AMBIGUOUS!

containers of SNM in the cargo compartments
How about an unauthorized opening?
He's missed the point of the logic. The procedures provide for keeping it locked & sealed & constantly under observation by 2 or more of the crew while moving!

if the SNM. Licens
the fixed site is sealed,
hardened, tamper indicating
containers, their detection
is not part of threat to
be considered.

BASIC CAPABILITIES

The basic capabilities essential to assure control and protection of SNM shipments against theft, diversion or sabotage while on transports are essentially to control access to the SNM, to assure sufficient initial physical protection and, if needed, to provide effective response to an attempt to steal or sabotage SNM. These capabilities are developed in the following discussion.

- 1. Access Control. Assure that only authorized personnel and materials in authorized quantities are admitted on transports.

The essential elements of capability 1 would include procedures:

- a. For establishing job functions that ^{would limit} ~~should permit~~ access to transports, transfer point storage areas or escort vehicles to auth. personnel
- b. To limit access to those persons in authorized job functions.

Such procedures should take into account access to transports and storage areas prior to their being used for SNM transport or storage and particularly during maintenance. This should also include escort or driver surveillance procedures during stops in-transit.

- c. For assuring the trustworthiness of personnel having access to SNM.
- d. To verify and confirm the identity of material placed in or removed from the transport or storage area.
- e. To assure that there is a search for unauthorized materials already in the cargo compartments of transports or transfer storage areas that could assist in the theft or sabotage of the SNM. *poorly worded*
- f. To lock and seal material containers, cargo compartments and storage areas.
- g. To verify and confirm that the locks and seals of material containers, cargo compartments and storage areas have not been tampered with.

What are the characteristics of the program to be...
Cite talk about subject kind of protection as discussed

To what degree do you want to detail data/...
Cite report to each of the...
Other possible elements

What is the sabotage risk?

do not understand?

h. To provide for initial detection of attempts to gain unauthorized access to SNM or introduce unauthorized materials on transports.

2. Physical Protection. Assure that effective physical security measures are present in order to prevent an attempt to steal SNM by stealth or by force and to prevent sabotage.

The essential elements of capability 2 would include:

- a. Provisions for hardened containers and vehicles for land transportation and hardened containers for air and sea transportation.
- b. Proper training, arming, communications and assigning appropriate numbers of drivers and escorts for in-transit shipments.
- c. The use of temporary barriers to isolate transports while stopping in unprotected areas.
- d. Provision for initial detection of unauthorized conditions or immediate threat through use of adversary information, surveillance, electronic detection systems and alarms.
- e. Route selection with minimum stops and transfer points.

Is this the only measure to be taken in driving stops or storage?

3. Response. Assure timely detection and effective response to an attempt to steal or sabotage SNM.

The essential elements of capability 3 would include:

- a. Provisions for an immediate response force of escorts to delay or defeat any adversary force attempting to steal or sabotage SNM.
- b. Establishment of effective communications systems and contingency procedures with LLEA and transfer point security forces.
- c. Establishment of communications systems and procedures with a fixed base to record transport location and permit continuous monitoring of transport status and location.

d. Provisions for continuous surveillance and communications during adversary engagement to provide for updated information to response forces.

e. Provisions for passive response to include immobilization and inundation with irritants or obscurants.

f. Provisions for material recovery in the event SNM control is lost.

+ 11
C. South

COMMENTS ON "RESPONSE CAPABILITY" DRAFT

GENERAL - The draft as it is currently written does not clearly delineate several capabilities that are integral to effective response. They have to do with (a) deployment for timely mobilization, (b) protection of the guard force in such deployments, (c) quality and availability of defensive equipment, (d) quantity of guards vs. capability of (LLEA) offsite response forces and timeliness of support when requested, and (e) motivation of the onsite force to protect the SNM (use of deadly force if necessary).

While parts of several of these can be inferred from different sections of the draft, it is not at all certain that they will be. To preclude this possibility we should specifically include them. The "Response Plan" section might be a place to start. As worded now, it says very little of substance and is referred to in the other sections.

Deployment measures should be called for (in some part of the document) which (a) provide timely mobilization of onsite response forces, including vehicular support if site topography requires it, and (b) prevent neutralization of the guard force before arrival of the offsite response force.

Protection of the guard force in their deployments should be required which includes at least (a) hardening of the onsite alarm

stations against small arms fire, and (b) secure silent duress alarms between alarm stations and guard posts. These measures, plus others, should make unlikely the overrun or interdiction of response forces before they could engage in an assault.

Qualitative aspects of the defensive capability during an engagement need to be stated, such as types of arms and their availability when needed, training and exercises, existence of a clearly defined chain of command, etc.

Quantitative aspects of the defensive capability for engagement need to be stated in context with probable LLEA support when requested. These include numbers of guards, numbers of defensive weapons, range of time delays from LLEA request to onsite appearance, and the geometry of the site defense problem. The point to be stressed is the trade-off required between the site specific ~~specific~~ and other variables to satisfy a generic protection requirement. Time delays must be included as well as the kind of external support realizable.

Guard force motivation is an essential element of the response capability, particularly with regard to the use of deadly force, if needed, to defend against theft of SSNM, and should be so stated. Without this ingredient the effectiveness of a guard force to ward off a determined violent assault is in question.

In summary, each of the above needs to be worked into the draft narrative somewhere and should be explicitly worded so the reader has no doubts of the meaning intended.

SPECIFIC - Two kinds of forces are called out, reaction forces and response forces, but not defined. Apparently the former is the guard force and the latter the LLEA. Correct? The introduction should state that safeguards response is a possibly two pronged affair and introduce/define these terms at that time (since it pertains to several of the sections).

Also all of the other four capabilities have referenced the response capability section in the area of response to reported intruder alarms or other unauthorized activity detections. Now is the time to define for one and all what we mean by "respond in an effective and acceptable manner". Again, it should be done in the introductory section.

Additional detailed comments are offered via a marked up copy which is attached, although I do not believe a draft update with only these comments included would constitute an acceptable product. A major rewrite is required along the lines of the general comments above.

P. South

Note - "effective and acceptable" must be defined.

~~C. Smith~~
DRAFT 3/2/77
APoltorak/meb

ENCLOSURE

Response Capability

The safeguard system shall provide a response capability that will be compatible with, and complete in an effective and acceptable manner, the ~~five~~ ^{four} basic functional capabilities described in Sections .

The following safeguard subsystems and functions are necessary to assure the ~~detection~~ ^{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 of the safeguard system; *to protect against theft of SNM.*
- b) assess information collected by the detection systems and designate appropriate reaction/response activities based on the response plan;
- c) react or ^{request LLEA} implement response activities based on the assessment;
- d) provide command and control ^{of} ~~to~~ reaction and response forces for direction and coordination of activities to assure an effective and acceptable response; ~~and~~
- e) provide liaison with LLEA and other security organizations to ^{assess capability for} assure their assistance to reaction forces in cases of needed support and ^{to assure their likelihood of support, and} emergencies.
- f) *establish and maintain a documented and clearly stated chain of command with specific restrictions, authorities and authority stated to cover the spectrum of conditions from normal to emergency, including engagement of an adversary.*

SEC GENERAL
2/2/2015

2. Response Plan: The licensee shall establish response plans to cover all anticipated ^{situations involving an apparent or real adversary force} ~~non-routine situations~~, consisting of:

- a) assessment procedures which provide methodology for evaluating detected situations based on the established ^{safeguards} authorizations;
- b) alternative courses of action to be employed by the security organization based on the detection and assessment function outputs for all anticipated ^{adversary related} ~~non-routine~~ situations; and
- c) procedures for when and how to interact with the LLEA for assistance. ^{and who is so authorized.}

3. Equipment and Facility Design: The licensee shall provide ^{defensive} ~~protective~~ equipment for the security organization and incorporate ^{protective} ~~facility~~ design measures that will:

- a) ^{SUPPORT} ~~assist~~ the performance of the assessment and response activities;
- b) facilitate the implementation of response activities by providing for ^{effectiveness} ~~ease~~ of movement and physical protection of reaction/response activities (provide primary and secondary alarm stations to facilitate ^{redundant} ~~assessment~~ and command, control and communication activities);
- c) minimize exposure of reaction/response force personnel ^{to adversary fire} and
- d) minimize opportunity for access to SNM ^{during deployment} ~~of the reaction/response forces.~~

4. Communications: The licensee shall provide communications facilities and equipment for the security organization that will:

- a) interface with the detection capability to permit rapid and accurate transmission of detections and collected information, for assessment purposes and to notify reaction response forces;
define reaction force
- b) notify LLEA of need for assistance, as identified in the response plan;
SG problem assessments or request their
- c) coordinate on-site reaction and response forces with multiple, independent communication links; and
activities
- d) alert appropriate authorities (key personnel/appropriate agencies) via timely communications of adversary related non-routine situations as identified in the response plan.
define

*How many?
3?*

Note - Unlike the other two capabilities, the response matter is primarily a "military" type problem - heavily dependent on quacks and/or police, weapons, tactics, etc. Why don't we use the kind of language and its terminology which has precise meaning? It would improve communications with the resources, or have it, to include senior people of this type in charge of the security organizations.

7 March 1977

Note to C. South

RESPONSE CAPABILITY NARRATIVE -- DRAFT DATED MARCH 2, 1977

We cannot comment meaningfully on the subject draft until we understand the relationship, if any, of the proposed "Response Capability" to the licensee safeguards contingency plans for dealing with threats, thefts, and sabotage relating to special nuclear material and nuclear facilities resulting from all activities licensed under the Atomic Energy Act of 1954, as amended.

For your information, the Commission will, during the week of March 28, act on the proposed rule requiring licensee safeguards contingency plans, a copy of which was given to L. J. Evans, Jr. with a suggestion that the "Upgrade" rule making take cognizance of this forthcoming regulatory requirement.

Justin

J. T. Long