I 57

TRW

21 January 1977

Mr. L. J. Evans, Jr.
Chief, Security Programs Branch
Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Mr. Evans:

Following our meeting of 18 January, we enclose some thoughts regarding the interdependence of the Basic Capabilities.

Yours truly,

Harvey J. Spiro

HJS:cs

Enclosures
cc: A. S. Poltorak

Some Thoughts on the "Basic" Nature of the Basic Capabilities

It would be conceptually appealing if each of the "basic" capabilities alone was sufficient to prevent theft of SNM, if it could be enforced perfectly. In fact, three of the five capabilities have that characteristic, namely BC2, BC3, and BC4.

BC2 - If all unauthorized "activities" and "conditions" could somehow be prevented, then by definition no one would do anything "wrong," nor would the integrity of the facility be violated.

BC3 - By assuring that no unauthorized or unconfirmed SNM leaves the facility, the threat of nuclear theft has been obviated.

BC4 - If a "perfect" accounting system could be devised, and impenetrable containment devices could be designed, then no further controls theoretically need be used, since the whereabouts of all forms of SNM is known, confirmed and authorized.

BC1 can prevent intruders from entering the PA, but is powerless against the threat of an insider.

BC5 is really the backup of muscle to all other capabilities, providing force if necessary to back up any other capability (limited, of course, to the six outsiders-one insider concept).

The problem is that none of these capabilities, "basic" or ancillary, can be implemented with 100% effectiveness, nor is any system - human, nor automated, nor any combination - totally foolproof. The magnitude of the downside risk of SG systems with loopholes makes it essential that redundant, independent, mixed mode systems be required.

An underlying assumption in all of these capabilities is the trust that something which is "authorized" is, by definition, okay. The implied confidence in the overseers of the facility, and the chain of communications and command by which their "authorization" is simultaneously jus divinum and pro bono publico must be looked upon as the ultimate built-in loophole, which must be monitored by the NRC.

BC2 - "Prevent Unauthorized Conditions and Activities" - OPTIONS

Decisions on three issues will shape the structure of Basic Capability 2. These should reflect the conceptual framework appropriate to the overall disaggregation plan.

A. Definition of the terms "conditions" and "activities"

The essense of BC2 is the monitoring of the environment within the facility. A semantic differentiation between "conditions" and "activities" only makes sense if it helps clarify or highlight the disaggregation of this capability.

Two alternate ways for doing this are:

1) Define "conditions" as involving equipment and grounds, and "activities" as involving people.
2) Define "conditions" to mean passive events, and "activities" to mean active events.

Either of these assumes that the SG elements used to monitor "conditions" (as defined) are different from those used to monitor "activities." If there is felt to be no need to emphasize such a breakdown, then the expression "conditions and activities" should not be dissected further.

B. Inclusion of a Containment Capability in BC2

why are these?

If BC2 is meant to include monitoring SNM containment devices, then BC2 is performing the containment function found in BC4, and the need for BC4 is brought into question. A strong case for retaining BC4 is presented in another document.

C. Inclusion of a SG System Quality Assurance Capability in BC2

The concepts of quality assurance, redundancy, PM, independence, etc. could be viewed as part of the "condition" monitoring of BC2, or they could be taken out and used in an overall set of constraints for all Basic Capabilities. Since they reflect qualities required for all Basic Capabilities, placing them in a list of overall constraints is conceptually "cleaner".