July 22, 1991

ALWR
ADVANCED
LIGHT WATER REACTOR

Document Control Desk
USNRC
Washington, D.C. 20555

SUBJECT: **Project No. 669 - Request for Additional Information on EPRI Advanced Light Water Reactor (ALWR) Requirements Document for Passive Plant Designs - Safeguards Branch (Tac No. 77871)**

REFERENCES: J. H. Wilson letter to E. E. Kintner, May 17, 1991

Gentlemen:

This is the response to the NRC staff request for additional information received with the referenced letter.

Please call John D. Trotter at EPRI, 415/855-2786, if you have any questions.

Sincerely yours,

E. E. Kintner, Chairman
ALWR Steering Committee

cc: James H. Wilson (with attachment)
G. Bockhold

EEK/GB/L64a/SEO

EPRI
ALWR Utility Steering Committee
3412 Hillview Avenue, Palo Alto, CA 94304 • Telefax: (415) 855-2774

A035
1/1

REQUEST FOR ADDITIONAL INFORMATION
EPRI ALWR UTILITY REQUIREMENTS DOCUMENT
FOR PASSIVE PLANT DESIGNS
SAFEGUARDS BRANCH

Chapter 10
NRC Question

910.39 The staff notes that Chapter 10 of Volume III (Passive ALWR) contains revisions addressing earlier staff comments on Chapter 10, Volume II (Evolutionary ALWR). In response to staff comments on applicability of requirements 4.5.4 and 4.6.3.1 to security equipment, the following statement was added to Section 10.2.1.8, "Site Security," on page 10.10-6 of Volume III:

> "The M-MIS for the plant security system shall meet the special requirements of Chapter 9, Section 5, as well as the applicable general requirements for an M-MIS In Chapter 10."

Although this statement clarifies that some requirements do not apply to security equipment, some ambiguities remain. Accordingly, the staff recommends that the referenced comments be further addressed for the passive ALWR by specifically identifying requirements which do not apply to security equipment. In particular, please address the following:

a. Inadvertent Actuation and Locking of Controls: Section 4.5.4 proposes that key-locks not be used for controls that may need to be actuated on a timely basis. The staff's position is that key-lock controls would be appropriate for some critical security system controls.

b. Dedicated wireless Communication System: Section 4.6.3.1 states a preference for telephone-type dial-up equipment. The staff's position is that hand-held radios are important for security patrols and response personnel.

Response

The plant security systems have numerous interfaces between plant equipment and personnel; consequently, the requirements in Chapter 10 relative to ensuring the functionality of the man-machine interface are applicable to the plant security systems. It is intended that

the controls and displays for the plant security systems be based on an identification of the functions and tasks and that good human factors design be applied. In fact, Section 5.2.13.2 of Chapter 9 specifically identifies the need for good human factors for the display of security information. The plant security systems, however, have some unique requirements which are specified in Section 5.2.11 of Chapter 9. As for other plant systems, the general requirements for the man-machine interface of Chapter 10 apply to the plant security systems unless modified by the system-specific requirements of Chapter 9. The two specific areas identified in the question (key-locked controls and communications) are discussed below.

Section 4.5.4 of Chapter 10 is intended to discourage (but does not preclude) the use of key-locked controls, particularly for controls which could be needed in a timely manner in an emergency. Some existing plants have many key-locked controls which are a potential source of operational problems. As explained in the rationale, there may be circumstances, particularly at unmanned locations, where a key-lock is the only practical method to ensure that a control is not operated inadvertently or by unauthorized personnel. The criterion of acceptability of key-locks indicated in the requirement, i.e., whether there may be a need for timely action in an emergency, would be equally applicable to plant security systems controls. In the case of plant security systems controls, however, the results of the sabotage vulnerability analysis required by Section 5.2.2.1 of Chapter 9 would also have to be considered by the designer of the M-MIS for the security systems in the selection of the method to prevent inadvertent or unauthorized operation for a particular control.

Section 5.2.11 of Chapter 9 includes specific requirements for plant security communications. These requirements will have to be met by the communications provided for the security forces. To the extent that the normal plant operational communication systems defined in Section 4.6 of Chapter 10 can meet these requirements, they can be used. However, it is evident that the requirements of 5.2.11 of Chapter 9 will require some special communication equipment dedicated to security-related uses, for example, the requirement for continuous communication with manned security stations and for a secure communication link between the main control room and major security control stations. The requirements of security-related communications are intended to be included in the communication analysis required by Section 4.6.2.2 of Chapter 10. In order to avoid the potential for misunderstanding as to the coverage of the

communication analysis, Section 4.6.2.2, Chapter 10 of Volumes II and III, will be modified to cite security-related communications and to identify the special requirements on those communications in Chapter 9.

- The first part of the first sentence of the first bullet item in the requirement will be modified so that it will read: "Detailed evaluation of the specific communication tasks that must be performed by operations, maintenance, and security personnel..."

- The following sentence will be added to the rationale: "The special requirements for the security-related communications are covered in Section 5.2.11 of Chapter 9."