DEFENSE NUCLEAR FACILITIES SAFETY BOARD

625 Indiana Avenue, NW, Suite 700, Washington, D.C. 20004
(202) 208-6400

April 29, 1994

The Honorable Charles B. Curtis
Under Secretary
Department of Energy
Washington, DC 20585

Dear Mr. Curtis:

Recognizing the safety significance of the development and use of standards in the design, construction, operation and decommissioning of defense nuclear facilities, Congress explicitly set forth in Sec. 312(a)(1) of the legislation establishing the Defense Nuclear Facilities Safety Board (Board) that: "The Board shall review and evaluate the content and implementation of the standards relating to the design, construction, operation, and decommissioning of defense nuclear facilities of the Department of Energy DOE--including all applicable Department of Energy orders, regulations, and requirements--at each Department of Energy defense nuclear facility."

In keeping with the provisions of Sec. 312(a)(1), the Board has followed the development and use of several orders and standards related to facility design and natural and man-made phenomena hazards. Our comments in this letter pertain specifically to DOE Order 5480.28 - "Natural Phenomena Hazards Mitigation," as well as to DOE Standards 1020-92 (Draft) - "Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities," 1021-93 - "Natural Phenomena Hazards Performance Categorization Guidelines for Structures, Systems and Components," 1022-92 (Draft) - "Natural Phenomena Hazards Site Characterization Criteria," 1023-92 (Draft) - "Natural Phenomena Hazards Assessment Criteria," 1024-92 - "Guidelines for Use of Probabilistic Seismic Hazard Curves at DOE Sites," and 1027-92 - "Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23 Nuclear Safety Analysis Reports." The order and standards are closely linked in content and intellectual underpinning, and form a system related to considerations of natural and man-made hazards. The following comments by the Board are amenable to the systems engineering approach where definition of requirements, integration, and analysis are performed early in the design process, while specifications or standards are in draft form.

We believe that the referenced order and standards have certain generic deficiencies, as follows:

a. The standards overemphasize new and largely probabilistic concepts and do not adequately use long accepted deterministic principles. A better balance should be achieved.

b. Definitive procedures to establish Safety Classes and Performance Categories have not been developed, nor has the relationship among Hazard Category, Safety Class, and Performance Category been clearly defined.

c. The standards are overly complex, lack clarity or completeness, and in many cases are not easily understood even by experts in the subject.

d. The proposed DOE grading of safety classification and performance goals and values have not been accepted by the engineering profession on a consensus basis.

e. Standards, guidance, and procedures for the design or assessment of electrical and mechanical systems that are consistent with the classification methodology to be used have not been developed.

f. No distinction is made between new and existing facilities, nor is there guidance on how the application of the requirements of the order and standards will differ for new or existing facilities.

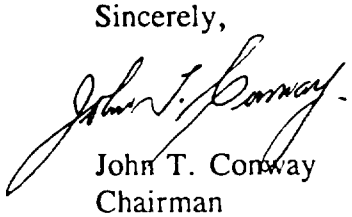
Further elaboration on the above is contained in Attachment A.

The Board believes that comprehensive reevaluation and streamlining of the referenced order and standards are necessary to resolve these issues. Any changes to the order and standards should reflect: 1) the use of widely-accepted engineering concepts for grading safety systems, 2) the development of technical approaches to and the integration of order and standards that can be more easily understood and implemented, and 3) the issuance of guidance for mechanical and electrical systems that is equivalent to that being provided for structures.

Pursuant to 42 U.S.C. § 2286B(d), the Board requests that DOE provide a report, within 60 days of receipt this letter, that details how these comments and those in Attachment A will be addressed, and provides a schedule for doing so.

The order and standards have been the subject of substantial dialogue among DOE staff, Board staff, and numerous subject matter experts. The Board is prepared to continue such interchange of views if it will assist DOE in further development and integration of the order and standards. In any case, the Board will continue to follow this development effort with intense interest. If you need any further information, please let me know.

Sincerely,



John T. Conway
Chairman

Enclosure (Attachment A)

cc: The Honorable Victor H. Reis, DP-1
The Honorable Tara O'Toole, EH-1
The Honorable Thomas P. Grumbly, EM-1

Attachment A

DNFSB Comments on DOE
Safety System Classification
and
Natural Phenomena Hazards Standards

1. DOE Standards

a. DOE Natural Phenomena Hazards (NPH) Standards generally embody a probabilistic strategy to provide a graded approach to safety and thus to safety system classification. While there is nothing inherently inappropriate in this concept, the approach, as currently implemented, suffers from two fundamental deficiencies:

(1) *The grading of safety classification* for Structures, Systems and Components (SSC) is tied to *specific* performance goals, where performance goals are defined in terms of the annual frequency of failure. Since the risk assessment community has not yet reached agreement on specific standards (preferably based on experience), which would provide a basis for adopting specific numerical values of these failure rates, the numerical grading of performance goals may be premature and require validation.

(2) The probabilistic approach has been more properly used to evaluate relative risks or relative measures of the occurrence of particular hazards, and only occasionally, when sufficient historical evidence exists, to determine an absolute value of risk. In the case of NPH events, there are insufficient historical data upon which to base an absolute value of risk as inherently used in these standards. Therefore, we believe that the probabilistic bases of these orders must be reexamined. They appear to represent a fundamental weakness in the underpinning of the safety system classification for NPH specifically, and system design related orders in general. An appropriate approach or policy statement needs to be defined on the use of the probabilistic methods throughout DOE.

b. DOE's current approach to characterization of seismic ground motion basically uses a probabilistic approach, and ignores the deterministic approach that has been the mainstay of the structural engineering profession up to the present time. While there is increasing use of probabilistic methods in the engineering profession, existing seismic data for low probability, large magnitude events are generally inadequate to provide even a statistical validation of the proposed probabilistic procedures for DOE sites in general and for sites in the eastern United States in particular. Thus, it is not prudent to rely solely on probabilistic principles. This issue is under consideration by Defense Programs. It is requested that any resolution of this issue be an integrated DOE effort with results made applicable to all DOE defense nuclear facilities.

c. Implicit in the development of the concept of the graded approach to safety is the assumption that some facilities pose more of a risk to the public and facility workers than do others, and that the consequences can be characterized as differential risk. However, DOE does not have an approved standard or guide which deals with the issue of quantifying risk. Some DOE contractors have used, as an acceptance standard, the assumed fission product release noted in 10 CFR Part 100.11(a) resulting in a reference dose of 25 rem at the site boundary. However, such use of 10 CFR Part 100.11(a) goes beyond the intent of its provisions. The value in question is intended to be used in establishing site exclusion boundaries for a facility or facilities incorporating specific safety systems on the assumption that these systems would function properly when called on. The development of a standard or guide, applicable to all DOE facilities to quantify the consequences of relative risk associated with natural hazard phenomena, and/or the reassessment of a policy for the protection of the public health and safety are considered essential by the Board. Further, this review should be based on consideration of the contribution of all facilities at a site to the overall hazard since a natural event such as an earthquake will likely affect all facilities within a site.

2. Safety System Classification

a. Safety System Classification, as defined in DOE Order 6430.1A, is in terms of three levels. Classification is assigned to safety systems with specific functions to protect the operator, public, and/or the environment. However, we have not found any evidence that the system of using three safety classes is or will be implemented at any DOE site. Most sites seem to be concentrating on developing a definition of a single safety class that includes only those systems whose failure could cause the radiological dose at the site boundary to exceed specified limits.

Under the current DOE concept, no safety system or hardening of structures would be necessary unless a predetermined site boundary dose would be exceeded following an accident or as a consequence of a severe natural phenomenon. This concept is stated to be based on 10 CFR Part 100. While 10 CFR Part 100 does address a site boundary dose for site selection, it also assumes that safety systems and structures that represent a "defense-in-depth approach" are prudently engineered into a facility from the outset, and not conditionally upon results of dose calculations derived from probabilistic methods. Defense in depth is still required to extend the level of safety beyond that indicated by analysis to provide a robust design that will behave safely for unanticipated events.

In the Board's opinion, the concept of safety system classification needs to follow logical thought processes which have evolved from commercial nuclear practice. 10 CFR Part 100 was used only to estimate the suitability of a site for a nuclear plant having a specified containment and specified safety features used to control pressure and temperature of the atmosphere in the containment following a hypothetical, non-mechanistic accident. In a sense then, it also determined the suitability of the containment and the pertinent safety features to be located at the site. Once the question of the suitability of this containment system was settled, 10 CFR Part 100 reference dose limits were not used further or to decide whether engineered safeguards should or should not be used.

The need for and suitability of safety features and engineered safeguards were then determined according to an assessment logic such as:

1) Is there defense in depth?
2) Would failure of these safeguards lead to unacceptable consequences?
3) Are there adequate measures to render failure suitably unlikely?

Acceptance dose limits are defined in EPA protective action guides, in recommended limits established by the International Commission on Radiation Protection and the National Commission on Radiation Protection, or are derived from ALARA considerations. They are <u>not</u> reference dose limits at the level of those discussed in 10 CFR Part 100.

The limitations in the commercial industry's Technical Specifications for nuclear plants are never derived using 10 CFR Part 100 considerations. They are based on deterministic analysis. Some are simply the result of ensuring adequacy of conduct of operations.

b. An item of interest to the Board is the apparent lack of use of the concept of defense in depth, used in the commercial nuclear industry, as it applies to safety classification of SSC. Specifically, it has been difficult to identify the application of safety classification to SSC's which prevent or mitigate the consequences of a postulated accident. We have not seen explicit evidence that this concept is definitely considered at DOE sites, yet clearly it should be.

c. It is not clear under what circumstances the current classifications will be applied, or if the application will be limited to new facilities or those undergoing major safety modifications. Therefore, we can envision the possibility of high hazard facilities where no safety classification of SSC has been implemented and the ability of SSC to mitigate potential accident conditions has not been evaluated. The Board is interested in determining when implementation of safety classification of all facilities according to current DOE standards will begin and how the application will proceed.

3. Performance Categorization

Performance Categorization is currently related to specific design requirements for NPH, such as earthquake, extreme wind, and flood. Performance Categorization is not considered for other design basis accidents and other external hazards, such as airplane crash, fire, and accidental explosion. Performance Categorization for external events must be considered. Other shortcomings are: 1) Performance Categorization for Design Basis Accidents does not include consideration of single failure criteria or active and passive failure criteria, 2) a clear relationship between Safety Class and Performance Category has not been developed, and 3) a clear relationship between facility hazard categories and Safety Classes and Performance Categories of SSC has not been developed.

4. Graded Approach

The graded approach to design of structures for NPH is treated in DOE Standard 1020-92. However, no standards exists within DOE that apply the graded approach to the design of electrical and mechanical systems and components. Guidance is urgently needed to deal with this issue, since without such definition, assurance that graded safety systems and components will achieve their design objective cannot be assured.

5. Standard 1020-92, "Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities"

Several fundamental concerns exist regarding this standard. First, the process proposed to achieve specified performance goals is complex and lacking in clarity for ease of application; the process needs to be simplified. Second, it is difficult to determine if the objective of the standard, i.e., the grading of facility design to match the hazard, will in fact, be achieved because of the numerous compensatory factors that are employed to grade the acceptance limit provisions of the standard. Third, it is not certain that all sites

and contractors will be able to understand and thereby correctly apply this standard. The standard addresses structures but does not provide equivalent guidance for the design or assessment of mechanical and electrical systems and components.

The standard is not written to allow the user to readily understand the conservatism and margin that will result with its use. Hence, blind application without a complete understanding of this standard's underpinning could lead to inappropriate and unconservative design bases. The standard needs to be revised to address the issues discussed above.

6. New versus Existing Facilities

The design of new facilities and the assessment of the adequacy of existing facilities are fundamentally different processes. In the design of new structural systems, for example, it is customary to estimate the various combinations of maximum design loadings and to choose resisting systems based on standard or minimum specified material/element properties, employing accepted safety margins. In the assessment of the adequacy of existing structures, it is customary to attempt to establish realistic loadings to which the structural system may be subjected and then to examine the available load and resistance on the basis of actual, potentially degraded, properties of the materials as best as they can be determined. The assessment of the margin of safety and a conclusion as to adequacy of the structure are then determined. However, DOE's current standards do not differentiate between the two processes; although such differentiation is clearly appropriate.