

September 8, 2000

The Honorable Bill Richardson
Secretary of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Secretary Richardson:

The Defense Nuclear Facilities Safety Board (Board) acknowledges your August 21, 2000 letter of notification that the Department of Energy (DOE) requires an additional 45 days to transmit the implementation plan for our Recommendation 2000-2, *Configuration Management, Vital Safety Systems*. The Board agrees that the draft plan developed to date can benefit from additional planning.

Section 315(e) of the Atomic Energy Act of 1954, as amended, provides that the Secretary “may implement any such recommendation (or part of any such recommendation) before, on, or after the date on which the Secretary transmits the implementation plan to the Board under this subsection.” In this regard, the Board notes that some limited, preliminary actions have been taken by DOE to define pre-requisites for tasks still in planning stages, e.g., identification of industry practices/standards relative to development of a contractor system engineer program. The Board suggests that DOE move more aggressively forward with similar initiatives such as the selection of the team for the Ventilation Systems Assessment, the initiation of the development of generic Criteria Review and Approach Documents (CRADs) for vital safety systems, and a review by Field Managers of current Functions and Responsibility assignments of both the Federal and Contractor personnel relative to vital safety systems. The Board urges DOE to take advantage of the authority granted under Section 315(e) to get more such preliminary actions underway.

Notwithstanding substantial Board staff discussions with DOE personnel responsible for drafting the plan, progress to date has been unduly slow. These discussions indicate that the leadership of the plan’s development does not clearly understand the basic thrust of the Recommendation. The Board offers further amplification in the enclosed material. Since your acceptance letter of April 28, 2000, did not reject any part of Recommendation 2000-2, the Board has assumed that the safety issue—Configuration Management of Vital Safety Systems—is to be fully assessed.

The basic thrust of the Board’s Recommendation—assessment of the operational readiness of vital safety systems—is direct and simple. The operational readiness of vital safety systems, their

continued surveillance, maintenance and configuration management are at the core of Integrated Safety Management (ISM). Both the contractor and the Federal workforces must recognize the pivotal role that these systems play in ensuring safety. The assessments to be done in response to Recommendation 2000-2 represent an important part of DOE's continued implementation of ISM throughout the complex. Full implementation of ISM cannot be considered accomplished until such vital safety systems are identified, responsibility is clearly established for their operational readiness, a satisfactory state of operational readiness is established, and a functional maintenance and configuration management system is put in place to ensure future readiness. Further elaboration of this core concept is described in the amplifying material enclosed. Ideas are also presented therein for closely coupling this 2000-2 effort with the ISM verification efforts that have been underway for the past several years. The Board sees no reason why the majority of the assessment effort required cannot be performed by resources, both contractor and Federal, that are already committed to ensuring safety. The potential for finding that upgrades of infrastructure may be required should not be cause for delaying assessments, nor should the accomplishment of verification goals set for September 2000 be cause for relaxation of continuing upgrade efforts.

It is the Board's view that developing a completely acceptable plan in the additional forty five days is not likely unless a change in momentum takes place. The Board has instructed its staff to continue its clarifying exchanges with the designated leadership of the implementation planning effort. DOE is urged to move expeditiously to complete the planning effort and to begin full implementation as soon as possible.

Sincerely,

John T. Conway
Chairman

Enclosure

c: Mark B. Whitaker Jr.

Recommendation 2000-2 Amplification

In performing its diverse missions, the Department of Energy (DOE) and its contractors use hazardous materials and processes. In doing so, DOE is required to protect the public, the workers, and the environment. DOE is fulfilling its environmental, safety and health responsibilities through its program of Integrated Safety Management (ISM) as defined by DOE Policy 450.4, *Safety Management*. A core function of ISM, “Develop and Implement Hazard Controls,” results in the establishment of a set of safety controls. Frequently these controls are in the form of systems and equipment designed and operated to protect the public, the worker, and the environment. Periodic surveillance, maintenance, and configuration management of these systems and equipment are required to ensure their dependability and reliability, to determine whether deterioration is taking place, and to identify technical obsolescence that threatens performance, safety, or facility operation. Full implementation of ISM cannot be considered accomplished until all such vital safety systems are identified, responsibility is clearly established for their operational readiness, a satisfactory state of operational readiness is established, and a functional maintenance and configuration management program is in place to ensure continued readiness.

DOE has developed the necessary standards and requirements to identify and implement both engineering and administrative controls to prevent accidental releases of hazardous materials or mitigate the consequences of such releases, should they occur. For accidental events that potentially could cause harm offsite or cause worker deaths or serious injury, such controls and the hazardous processes with which they are associated are described in Safety Analysis Reports (SARs) or equivalent documents. Limits on hazardous processes and the requisite availability of preventive and mitigative equipment are established as Technical Safety Requirements (TSRs). Such TSRs are made conditions for conducting the hazardous operations. These are included in “Authorization Agreements,” a set of safety measures mutually agreed upon by DOE and the contractor for operating high hazard facilities.

In addition, other controls to provide workplace safety and protection of the environment are defined through various process hazard analyses, job hazards analyses, environmental impact assessments and environmental permitting processes. These controls also become conditions for performing the hazardous tasks. Figure 1 illustrates basic elements of an “Integrated Safety Control Set” and the basic documents in which they are commonly described.

Figure 1

Authorization Protocols

INTEGRATED SAFETY CONTROL SET*				
	Safety Sector	Hazards Assessment	Hazards Controls	Authorization Protocol
Macro Level	Public	SAR and Graded Equivalents DOE Orders 5480.23	Technical Safety Requirements: \$ Design (Engineered Controls)	\$ Authorization Agreement - High/Moderate Hazards Facilities Category 1 and 2
	Worker Sector A	Process Hazards Analysis: 29 CFR 1910.119. Risk Management Program: 40 CFR 68	\$ Work practices and administrative procedures	\$ Authorizing Correspondence Moderate/Low Hazards Facilities Category 3 and 4
Micro Level	Worker Sector B	Job Hazards Analysis and Equivalents DOE Order 440.1 IG 440.1-1	Work Control Conditions: \$ Engineered Controls \$ Work practice and administrative procedures \$ Personnel Protective Equipment	\$ Rad Work Permits \$ Work Control Permits \$ Operation Procedure
	Environment	NEPA Documentation Permit Support Documents	Discharge Control: \$ Engineered features \$ Limits on discharges	Discharge Permits \$ air \$ water \$ solid wastes

This figure is taken from Board Report DNFSB/TECH-16

* Safeguards and Security not included

The Defense Nuclear Facilities Safety Board has emphasized that safety systems relied upon to protect the public, the workers, and the environment deserve special focus. Their design, procurement, fabrication, installation, operation, maintenance, and configuration management are at the core of ISM. Both contractors and the Federal workforce must recognize the pivotal role these systems play in ensuring safety and deploy their resources accordingly.

Much of the DOE nuclear complex was built years ago. Both the Federal workforce and the contractors employed by the government for maintenance and operation have turned over many times during the operational life of the facilities. Both process knowledge of many hazardous operations and the design basis of protective equipment and associated systems are often not current. While substantial updating of authorization basis documents is being accomplished under pressures of the ISM program, assessments by both DOE's internal safety management organizations and the Board's external safety oversight staff show that DOE's operating contractors are not always giving equipment designed to serve vital protective functions the attention their safety functions deserve. Confinement ventilation systems and fire protection systems are good examples. Recommendation 2000-2 seeks to have DOE systematically assess the readiness state of its vital safety systems and the effectiveness of their configuration management.

The acceptability of any plan offered by DOE in response to Recommendation 2000-2 will be based upon our evaluation of how well the objectives described above are likely to be satisfied. A set of tasks such as the following are visualized:

- Task 1. The identification of high hazard processes performed in all defense nuclear facilities, the vital safety systems/equipment providing protective functions, and the programs that support and preserve these systems (e.g., maintenance).
- Task 2. The targeting of Confinement Ventilation Systems in defense nuclear facilities for priority attention, using a special task force of subject matter experts to: (a) develop evaluation guidelines to be used in evaluating them, and (b) assess the operational ability to meet design requirements of a selected number of them, including the assessment of programs needed to preserve the system such as surveillance, maintenance, and configuration management programs.
- Task 3. The systematic assessment of the state of all systems/equipment upon which the safety of the site and its hazardous facilities depend (public, worker, and environment) and the adequacy of the resources applied to do surveillance, maintenance, and configuration management. Evaluation guidelines used in the Confinement Ventilation Systems evaluation will be used or adapted as appropriate. The assessments performed as required by DOE Policy 450.5, *Line Environment Safety and Health*

Oversight will be reviewed to ensure that the assessments provide adequate assurance that the systems maintain their ability to protect the public, the workers, and the environment.

- Task 4. The assessment of functions, responsibilities, and authorities relative to the caretaking of vital safety systems and the adequacy of the resources (number and expertise) dedicated to ensuring their state of readiness.

Establish contractor qualification requirements, and qualify system engineers, for hazardous processes and associated vital safety systems identified under Task 1. This will enhance the DOE's ability to ensure that engineering expertise is applied in all five functions of ISM.

Define Federal workforce expertise necessary to support, review, and oversee the contractor's system engineer program. Establish qualification requirements for, and qualify federal personnel, who will be relied upon for system expertise. This will enhance the DOE's ability to apply engineering expertise in all five functions of ISM.

- Task 5. The development of an upgrade program, prioritized to ensure reliable operation of systems that prevent or mitigate higher risk.

- Task 6. The resolution of the key HEPA filter issues identified in the Board's June 8, 1999 letter.

The Board remains open of course to any other alternative that would satisfy the objectives of the recommendation. The plan needs to not only define the work to be done but also the responsibility for doing it. The Board recognizes that the assignment of resources is the prerogative of DOE. However, the Board offers the following observations for DOE consideration. In keeping with one of the fundamental principles of Integrated Safety Management, the primary responsibility for maintaining vital safety systems in a reliable state of readiness rests with line management—more explicitly, those responsible for developing, reviewing, approving, and maintaining safety bases documentation, the safety controls and the related support programs. These responsibilities now lie principally with the DOE Operations Offices and their contractors. Hence, DOE Operations Office Managers and their contractors logically should be tasked to lead and perform the majority of the actions defined in the above tasks. In the interests of maintaining continuity and consistency with the Phase II verification effort, it would be highly desirable for the Field Managers to use the same individuals that led the Phase II verification assessments for them. Team membership, however, will require the selection of those expert in the vital safety systems being assessed.

While this recommendation is viewed as largely a field oriented effort, a continuing DOE-Headquarters line oversight of the effort is important to ensure appropriate consistency, accountability, and priority are maintained as these activities are conducted across programs and sites. Further, there

may well be subject matter experts in DOE-Headquarters that could well be brought to bear, for example, in the developing of uniform evaluation guidelines as was done for the *ISM Verification Team Leaders Handbook*. The use of an assessment approach similar to that put in place for the Phase II ISM verification will make it clear that 2000-2 tasks are in reality an extension of the ISM verification efforts.

DOE has been seeking to embed Integrated Safety Management as a fundamental responsibility of those in the line responsible for performing hazardous work. The Safety Management Integration Team (SMIT) was established as an ad-hoc group in response to Board Recommendation 95-2. Recommendation 2000-2 offers DOE a vehicle for facilitating the transition of the post-September 2000 ISM leadership efforts back to the Lead Program Secretarial Offices (LPSOs) and the Administrator of the National Nuclear Security Agency (NNSA). This could be accomplished by establishing for 2000-2 a steering group at headquarters, consisting of the Chief Operating Officers (COOs) of the Administrator of NNSA and the LPSOs, and the Principal Assistant Secretary for Environmental, Safety and Health (ES&H). The headquarters steering group could, for example, be made responsible for selecting expert team leadership and for creating assessment team guidance and generic Criteria Review and Approach Documents (CRADs) for vital safety systems. Such a steering group could monitor implementation plan progress, brief senior DOE management, and initiate course corrections as appropriate.