April 19, 2002

The Honorable Spencer Abraham
Secretary of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Secretary Abraham:

The Defense Nuclear Facilities Safety Board (Board) has received your letter of March 21, 2002, proposing a revision to the Department of Energy's (DOE) Implementation Plan for Recommendation 2000-2, *Configuration Management, Vital Safety Systems.*

This proposed revision describes a reasonable path forward for assessing the reliability and operability of confinement ventilation systems, and the Board accepts the revision. Further, the Board is pleased to hear that all DOE sites are planning to institutionalize Phase II assessment criteria into ongoing programs to ensure the continued viability of safety systems, including confinement ventilation systems. The Board looks forward to reviewing the plans developed by each of the sites to accomplish this task.

The Board notes, however, that the Phase II assessment schedule provided in a DOE letter dated April 4, 2002, reflects that Lawrence Livermore National Laboratory (LLNL) has not committed to conduct a Phase II assessment of the safety-class emergency power system in its plutonium facility (Building 332). The reason stated is that LLNL intends to downgrade the importance of the system to the lesser category of safety-significant.

Regardless of the classification of the system, the goal of Recommendation 2000-2 is to assess and understand the operability of vital safety systems. A comprehensive understanding of such systems is a prerequisite to maintaining their operability. The emergency power system at Building 332 is clearly such a system because, among other things, it powers the building's confinement ventilation system.

The Board considers LLNL's Building 332 confinement ventilation system as a fundamental barrier to the release of radioactive material. Confinement of material is especially important at LLNL given its proximity to the public. In a December 21, 1999 letter to DOE, the Board pointed out that LLNL's Building 332 safety-class emergency power system did not meet current safety-class standards. DOE's response of July 25, 2001, noted significant progress in addressing the Board's

concerns, and estimated that corrective actions would be completed by the end of 2002. A recent review of the Building 332 electrical system conducted by the Board's staff concluded that although some compensatory measures were taken, LLNL had not corrected previously identified deficiencies related to single-point failures. A Phase II review would systematically identify vulnerabilities with the existing system and provide the system engineers with important data to prioritize the system vulnerabilities.

Additionally, during the review at Building 332, the Board's staff discovered that changes made to DOE Order 420.1, *Facility Safety*, in October 1996 were not included in the Contractor Requirements Document (CRD) for this Order, or the LLNL contract. The omitted requirements invoke specific national and industry standards that form the basis for design criteria for safety-class electrical systems. Discussions with your staff revealed that this was an inadvertent omission, and that the CRD would be corrected as a part of a change to this Order that is already being processed. However, LLNL personnel indicated that there were no plans to apply the industry standard requirements associated with safety-class emergency power systems unless such a requirement was inserted in the LLNL contract. This position is untenable without equivalent design criteria or assessment criteria defined for a safety-class emergency power system.

The Board considers that additional National Nuclear Security Administration senior management attention is required to ensure that LLNL satisfies the intent of Board Recommendation 2000-2. Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board would like to be briefed within 30 days of receipt of this letter on DOE's and its contractor's path forward for addressing the issues outlined in the enclosed issue report.

Sincerely,

John T. Conway
Chairman

c: The Honorable Everet H. Beckner
Mr. Edward Blackwood
Mr. Mark B. Whitaker, Jr.
Mrs. Camille Yuan-Soo Hoo

Enclosure

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

April 11, 2002

MEMORANDUM FOR: K. Fortenberry, Technical Director

COPIES: Board Members

FROM: A. K. Gwal

SUBJECT: Emergency Power System at the Lawrence Livermore National Laboratory's Plutonium Facility (Building 332)

This report documents a review by members of the staff of the Defense Nuclear Facilities Safety Board (Board) of the Emergency Power System (EPS) at Lawrence Livermore National Laboratory's (LLNL) Plutonium Facility (Building 332). The report, based on a review conducted at LLNL by staff members W. Andrews, B. Broderick, and A. K. Gwal on March 26–28, 2002, also reflects the results of a follow-up review of documents provided to the staff. The review at LLNL included discussions with site personnel and a walkdown of critical components of the emergency power system.

Background. On December 21, 1999, the Board sent a letter to the Acting Assistant Secretary for Defense Programs of the U. S. Department of Energy (DOE), portions of which detailed deficiencies within the EPS at Building 332. DOE responded to the Board's letter on July 25, 2001, and submitted LLNL's corrective action plan for addressing the issues identified by the Board. The Board directed its staff to assess the progress and current status of LLNL's corrective action plan and to evaluate the technical basis for the LLNL arguments against the performance of a Phase II assessment of the EPS as part of the Board's Recommendation 2000-2, *Configuration Management, Vital Safety Systems.*

Emergency Power System. The Board's staff evaluated the design of the electrical distribution system for Building 332 with emphasis on the EPS, which is designated as a safety-class system in the building's current Safety Analysis Report (SAR). The safety-class EPS at Building 332 provides emergency power to the safety-class Glovebox Exhaust System, Down-Draft Ventilation System, Room Exhaust System, Room Supply System, and Fire Protection System. The EPS consists of two emergency diesel generators, automatic transfer switches, and an uninterruptible power supply for vital facility emergency systems. The staff identified the following issues regarding this safety-class EPS.

Safety Classification of the Emergency Power System—The main issue outlined in the Board's letter of December 21, 1999, to DOE was the vulnerability of the Building 332 EPS to single-point failures that would trigger the subsequent loss of one or more of the four separate downstream safety-class systems requiring emergency power. The staff observed that single- point failures still exist in the present EPS, including the example explicitly cited in the Board's previous letter. Furthermore, it appeared that the laboratory has made few tangible attempts to remedy system vulnerabilities associated with single-point failures.

This lack of progress with regard to the issue of single-point failures appeared to be driven by the laboratory's stated desire to reconfigure the ventilation/confinement methodology for Building 332 such that this safety-class system would be able to perform its intended safety function even if primary and emergency power were lost. LLNL believes that this transition from an active to passive ventilation/confinement control strategy would make it possible to downgrade the safety classification of the EPS from safety-class to safety-significant. While this approach may ultimately prove to be acceptable, there is currently no comprehensive plan or schedule for its implementation. Until this change can be implemented the EPS for Building 332 is a safety-class system and should be treated accordingly.

Criteria for the Safety-Class Emergency Power System—The EPS is assigned a safety-class categorization in the safety basis for Building 332. Requirements as to what the safety-class designation should entail are set forth in DOE Order 420.1, *Facility Safety*, and its accompanying Implementation Guide. However, the requirements contained in the Order are not carried over to the Contractor Requirements Document (CRD) in their entirety. Specifically, the following paragraph from the Order related to facility safety-class electrical systems is missing from the CRD:

> *Facility safety-class electrical systems shall be designed to the basic approach outlined in Section 5.2.3 (Electrical) of the "Implementation Guide for Non-reactor Nuclear Safety Design Criteria and Explosives Safety Criteria."*

Standards listed in Section 5.2.3 of the Implementation Guide provide specific requirements for the electrical safety-class system, such as single-failure criteria, independence of equipment and circuits, equipment qualification, and connection of non-safety loads to safety busses.

Because the CRD does not contain the requirements relating to safety-class electrical systems found in DOE Order 420.1, LLNL personnel have taken the position that safety-class electrical systems do not have to meet the criteria set forth in the Order. Some components of the safety-class criteria that are not being met are single-failure criteria, independence of equipment and circuits, and connection of non-safety loads to safety busses.

Regardless of the omission of mandatory standards and requirements pertaining to safety-class electrical systems in the CRD, LLNL remains responsible for developing a clear definition of what attributes and characteristics of a safety-class electrical system are necessary and sufficient for it to be appropriately considered safety-class. Furthermore, any broad deviation from consensus industry standards, especially those mandated by DOE Order 420.1, that tend to degrade the performance of required safety functions should have sound technical justification.

Safety Assessments and Identification of System Deficiencies—Typically, the components of safety-class power systems and their associated design, operating, and maintenance documents are required to be marked or labeled in a distinctive manner. LLNL's engineering documentation, however, such as electrical one-line diagrams, panel load schedules, and other such documents, do not distinguish between safety-related and non-safety-related equipment in any way. As a result, identifying deficiencies related to the existence of single failure points and degradation of safety-class systems due to the connection of non-safety loads becomes a tedious and difficult process for the system engineers. The Board's staff reviewed several of the electrical load schedules and identified numerous instances in which non-safety loads are connected to safety busses. These conditions have the potential to degrade the safety-class electrical system.

LLNL has performed only a very limited high-level vulnerability assessment that it used to conclude that single-point failures either did not exist or were an acceptable risk. However, the conclusions of this assessment are based on assertions that lack technical validity. As an example, the vulnerability study concludes that the loss of ATS-07, an automatic transfer switch that directs power from both backup emergency generators to all downstream safety loads, is not a single-point failure since normal power will be available. This is an inappropriate assumption since emergency power is only called upon in the event that normal power is unavailable. A more technically sound understanding of the vulnerabilities associated with the Building 332 EPS could be gained by conducting a thorough and methodical system assessment including analysis of all emergency busses and loads, both high- and low-level. The Board's staff also believes it would be advisable for LLNL to update the electrical calculations to reflect currently installed conditions and evaluate the 40-plus-year-old safety-class cables to identify any potential age-related degradation.

Conclusion. The staff observed at LLNL a fundamental lack of understanding of system vulnerabilities in the Building 332 EPS. The staff believes a Phase II assessment of this EPS would enhance the overall understanding of and confidence in this vital safety system. It would also ensure that improvements that may ultimately be deemed necessary could be planned and implemented in a prioritized and risk-informed manner.