

January 8, 1999

The Honorable Bill Richardson
Secretary of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0104

Dear Secretary Richardson:

The Defense Nuclear Facilities Safety Board (Board) and its staff have been following the efforts of the Department of Energy (DOE) and its contractors to address potential problems in microprocessor-based systems because of year 2000 date issues. Observations from recent staff reviews of the year 2000 programs at Lawrence Livermore National Laboratory and the Rocky Flats Environmental Technology Site are enclosed for your consideration. Staff observations of the Oak Ridge year 2000 program were forwarded to DOE on November 24, 1998.

The Board is concerned that DOE has provided inadequate direction to the operators of its defense nuclear facilities with regard to evaluating safety-related systems for year 2000 compliance. In accordance with the direction from DOE headquarters, systems classified as mission-essential receive the highest priority and the closest scrutiny by headquarters. However, the initial definition of mission-essential systems did not specifically address the safety significance of equipment and was interpreted by many sites to apply to such systems as business management and payroll. For many sites, systems that protect the health and safety of the public are not classified as mission-essential. As a result, efforts to bring these systems into compliance receive less scrutiny and review than efforts directed toward certain business systems, which, though important to DOE's mission, do not have the potential for immediate impact on public health and safety as do the safety-related systems.

Although DOE should continue with current plans for mission-essential systems, the Board is concerned that the lack of emphasis on safety-related systems on the part of DOE headquarters may be encouraging many DOE sites to expend scarce resources on bringing business systems into compliance as soon as possible at the expense of similar efforts for important safety-related systems. Therefore, pursuant to 42 U.S.C. § 2286b(d) the Board requests DOE to report on the status of safety-related equipment evaluations for year 2000 compliance at all defense nuclear facilities as detailed in Enclosure 1.

Sincerely,

John T. Conway
Chairman

c: Mr. Mark B. Whitaker, Jr.
Ms. Jesse Roberson
Dr. James Turner

Enclosures

Enclosure 1

Reporting Requirements on Year 2000 Compliance for Safety-Related Systems at the Department of Energy's Defense Nuclear Facilities

February 15, 1999

- Identification of safety-related systems that may have year 2000 compliance issues
- Schedule for remediation, testing, and independent verification and validation

March 31, 1999

- Update on progress for completing year 2000 program for the safety systems that have been identified

April 30, 1999

- Status of continuity and contingency plans for safety-related systems and external effects that may compromise safety-related systems

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

December 14, 1998

MEMORANDUM FOR: G. W. Cunningham, Technical Director

COPIES: Board Members

FROM: T. Davis

SUBJECT: Year 2000 Compliance for Safety-Related, Microprocessor-Based Systems at Lawrence Livermore National Laboratory

This memorandum documents a December 2–3, 1998, review conducted at the Lawrence Livermore National Laboratory (LLNL) by the staff of the Defense Nuclear Facilities Safety Board (Board). The staff reviewed the laboratory program for ensuring that date-related problems associated with the year 2000 do not adversely affect microprocessor-based systems. The particular focus was on how that program was implemented for safety-related systems at the LLNL plutonium facility (Building 332).

As with other Department of Energy (DOE) sites, the primary emphasis of the LLNL year 2000 program is on mission-essential systems. Unfortunately, safety-related systems at LLNL are not identified as mission-essential because of the initial definition provided by the DOE headquarters Year 2000 Project Office, which did not necessarily include safety-related systems. This lack of emphasis on safety-related systems is causing LLNL and other DOE sites to expend scarce resources on bringing business systems into compliance as soon as possible, while not undertaking appropriately expedited efforts for important safety systems.

Awareness and Assessment. The LLNL year 2000 program is organized under the oversight of a site coordinator. The coordinator chairs a year 2000 task force, which includes a representative from each laboratory directorate. The task force representatives are responsible for ensuring that the systems under their directorate are evaluated for year 2000 compliance, and they use facility points of contact to conduct these activities. However, these representatives and their points of contact receive little guidance and no training on acceptable methods for identifying and evaluating systems.

Specifically, for the Defense and Nuclear Technologies Directorate, which is responsible for Building 332 systems, the directorate representative's written plan for assessing year 2000 compliance emphasizes computer systems and provides no guidance on identifying and resolving issues for embedded microprocessor-based systems. Based on the systems currently identified for Building 332 and a staff tour of the facility, there appear to be many important systems that have not been identified and assessed for year 2000 compliance. Building 332 management stated that they intend to complete their review for safety-related systems before reviewing programmatic systems. However, the review of the safety-related systems appears to have started in November 1998, and no documented plan or schedule currently exists for the remaining systems. Some of the programmatic equipment in Building 332, which will be the last equipment reviewed in Building 332, provides important safety functions, such as furnace and melter control for plutonium processing.

Remediation, Testing, and Validation. There is currently no clearly defined program in place at LLNL for testing and validation of safety-related systems that are not classified as mission-essential (e.g., all safety-significant and safety-critical systems in Building 332). Few if any safety verification and validation efforts have been completed to date for these systems. After extensive discussions, Building 332 personnel agreed that it would be prudent to subject safety-related systems in Building 332 to at least the same level of rigor applied to mission-essential business systems (e.g., payroll). While LLNL expects to meet the March 31, 1999, Office of Management and Budget deadline for mission-essential systems, the staff is not convinced that the independent verification and validation of the safety-related systems in Building 332 can be accomplished in this time period.

Contingency Planning. Given that every noncompliant system with health and safety impact may not be identified or successfully upgraded before the year 2000, appropriate contingency planning will be essential to ensure safe operations during the transition to that year. LLNL appears to be identifying appropriate compensatory measures necessary to ensure safe operations. Although most specific plans and procedures have not yet been developed, LLNL intends to have all necessary plans and procedures in place before 2000.

Staff Path Forward. The staff will follow up with LLNL personnel to further evaluate their progress and performance in assessing, upgrading, testing, and validating facility and programmatic equipment in the plutonium facility. The staff will continue conducting similar reviews at other DOE sites to evaluate the overall performance of DOE in assessing the year 2000 compliance of safety-related equipment in the defense nuclear complex.