

John T. Conway, Chairman
A.J. Eggenberger, Vice Chairman
Joseph J. DiNunno
Herbert John Cecil Kouts
John E. Mansfield

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

625 Indiana Avenue, NW, Suite 700, Washington, D.C. 20004-2901
(202) 208-6400

98-0003961



November 24, 1998

The Honorable Victor H. Reis
Assistant Secretary for Defense Programs
Department of Energy
1000 Independence Avenue, SW
Washington, D.C. 20585-0104

Dear Dr. Reis:

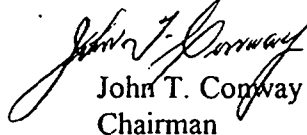
The Defense Nuclear Facilities Safety Board (Board) and its staff have been following the programs initiated by the Department of Energy (DOE) and its contractors to address potential problems in safety-related microprocessor-based systems. During a recent review of the year 2000 program at the Oak Ridge Y-12 Plant, the Board's staff made several observations regarding areas for improvement in the program. These observations are enclosed for your consideration and action, where appropriate.

Since it is not possible to foresee every potential problem that might arise, appropriate contingency plans and compensatory measures need to be evaluated for systems that cannot be brought into compliance before 2000.

The Board also calls your attention to the fact that appropriate emphasis has not yet been given to potential safety impacts on facilities and equipment associated with Enriched Uranium Operations (EUO). At the time of the staff review, EUO had not completed an initial assessment of facilities and equipment to identify potential year 2000 issues. The Board encourages the Oak Ridge Operations Office and Lockheed Martin Energy Systems to work closely with other DOE sites to incorporate lessons learned from other year 2000 programs across the DOE defense nuclear complex.

The Board will continue to follow the progress of the year 2000 program at Oak Ridge and would appreciate being kept informed of actions taken to address safety implications of the year 2000 problem at defense nuclear facilities.

Sincerely,


John T. Conway
Chairman

c: Mr. Mark B. Whitaker, Jr.
Mr. Gene Ives
Mr. James Hall

Enclosures

DEFENSE NUCLEAR FACILITIES SAFETY BOARD
Staff Issue Paper

October 9, 1998

MEMORANDUM FOR: G. W. Cunningham

COPIES: Board Members

FROM: W. White

SUBJECT: Year 2000 Compliance for Safety-Related Microprocessor-Based Systems at the Oak Ridge Y-12 Plant

This information report documents a September 11, 1998, review of the year 2000 compliance status for safety-related systems at the Oak Ridge Y-12 Plant. This review was performed on September 11, 1998, by a member of the staff of the Defense Nuclear Facilities Safety Board (Board), W. White. Year 2000 compliance has been identified as a potential problem for any system that uses microprocessors. The ongoing effort by the Department of Energy (DOE) to evaluate its systems for year 2000 compliance has received consistently negative reviews from the General Accounting Office, the Office of Management and Budget, Congress, and others. This scoping staff review assessed the program in place at Lockheed Martin Energy Systems (LMES) for evaluating Y-12 Plant equipment with regard to year 2000 compliance.

Awareness and Assessment. The LMES year 2000 project is organized under the LMES Chief Information Officer, but it includes significant support from the various Y-12 Plant line organizations. The project team raises awareness of the year 2000 issue through constant communication with Y-12 line organizations; the team also coordinates efforts related to mission-essential systems and centrally managed software systems, such as payroll and accounting systems. Senior LMES management personnel assist in stressing the importance of the project through internal correspondence to the various line organizations.

Although the year 2000 project team coordinates the LMES efforts at evaluating year 2000 compliance, the identification and assessment of most individual plant systems is being completed by the responsible line organization. As microprocessor-based equipment is identified by the line organizations, it is entered into a database that is maintained and tracked by the year 2000 project team. The project team has not evaluated the quality of the various assessments conducted by the line organizations, and they have not provided any detailed direction to the line organizations on acceptable methods for verifying year 2000 compliance. In many cases the identification and assessment of equipment is being completed by personnel without a good understanding of the year 2000 issue. The assessment mechanisms being used by the line organizations range from vendor phone calls to extensive software testing. The only organization that has not completed this initial assessment is Enriched Uranium Operations (EUO), which is responsible for some of the more hazardous operations at the Y-12 site.

There are few systems at Oak Ridge that have been identified as susceptible to the year 2000 problem and whose failure could impact public or worker health and safety. The systems identified include the fire protection system, the emergency notification system, and the supervisory control and data acquisition system that monitors electrical power at Y-12. These systems are in the process of being upgraded or replaced before the year 2000, although they may not be compliant before DOE's target implementation date of March 31, 1999. Given the variable quality of assessments completed by the line organizations (and the absence of any assessment by EUO), it is not clear that all safety-related microprocessor-based systems have been identified.

Remediation, Testing and Validation. The LMES year 2000 project team is responsible only for the remediation, testing, and validation of mission-essential or centrally managed software systems. The remediation, testing, and validation of most individual plant systems that have been identified as year 2000 noncompliant are completed by the responsible line organization. As with the assessment of the equipment, there is no detailed guidance from the year 2000 project team on requirements for bringing noncompliant equipment into compliance. There is also no review by the year 2000 project team of the quality of the efforts being made by the various line organizations to upgrade noncompliant equipment. The level of effort for testing and validation of repaired or upgraded equipment ranges from simply changing a few dates and observing the results to performing extensive software testing with the assistance of vendor technical support. Documentation of the testing and validation results is limited.

Contingency Planning. As it is unlikely that every noncompliant system will be identified and successfully upgraded before the year 2000, it may be advisable for DOE sites to consider contingency planning to ensure safe operations during the transition period. Appropriate compensatory measures need to be in place for systems that cannot be brought into compliance before 2000; for off-site support systems, such as electrical power, over which the site may have little control; and for failures that cannot be anticipated. These measures could range from encouraging operators to watch carefully for possible problems during early January 2000 to actually limiting operations during that period so that any possible occurrences would be easier to manage. There has been very little contingency planning to date by either the LMES year 2000 project team or the various line organizations at the Y-12 site.

Staff Path Forward. The initial review of the LMES year 2000 project at Oak Ridge is the first in a series of DOE site reviews to be conducted by the Board's staff. The staff will follow up with Oak Ridge personnel to further evaluate the performance of the various line organizations in assessing, remediating, testing, and validating plant equipment that is not known to be year 2000 compliant. The staff will also conduct 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.