

John T. Conway, Chairman
A.J. Eggenberger, Vice Chairman
John E. Mansfield

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

625 Indiana Avenue, NW, Suite 700, Washington, D.C. 20004-2901
(202) 694-7000



March 25, 2003

The Honorable Linton Brooks
Acting Administrator
of the National Nuclear Security Administration
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0701

Dear Ambassador Brooks:

Since issuing Recommendation 2002-1, *Quality Assurance for Safety-Related Software*, the Defense Nuclear Facilities Safety Board (Board) has continued to review the implementation of existing software quality assurance (SQA) procedures at defense nuclear facilities. The Board notes that during the past year, BWXT Pantex has undertaken significant actions to develop and implement a rigorous SQA program that specifically addresses safety-related software. During a recent review at Pantex, however, the Board's staff observed significant problems with safety-related software systems for which development began prior to the BWXT Pantex initiatives to improve SQA.

The new Interactive Electronic Procedures (IEP) being developed at Pantex are intended to provide on-line development, approval, and use of nuclear weapons procedures. The Board notes that successful implementation of the IEPs, identified by BWXT Pantex as safety-class software, may be jeopardized by observed inadequacies in software engineering practices. Further, although IEP implementation is scheduled to occur this year, key SQA requirements specified in Pantex Plant Standard 1875, *Software Quality Life Cycle*, have not been met. Although the use of IEPs has the potential to enhance conduct of operations at the Pantex Plant, the Board is concerned that inadequate software engineering practices could result in faulty procedures.

A number of problems were also observed with the new Move Right material tracking system software. The Move Right system has been identified by BWXT Pantex as safety-class software because it is relied upon to ensure that design basis assumptions are protected. The following are examples of system problems noted:

- On at least one occasion, Move Right did not accurately reflect the location of nuclear material because data entry errors in a non-safety-related software system propagated into Move Right databases.

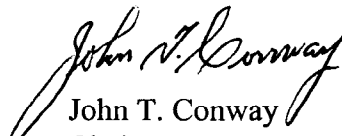
- Move Right's awkward human-machine interface, coupled with inadequate training, has resulted in special nuclear material being moved without authorization.
- Move Right is unable to manage certain high-explosive-only material.
- Move Right requires manual intervention to reconcile material accountability for all assembly/disassembly operations.

These problems can and have resulted in material control and accountability issues. While the Move Right system provides the opportunity for an improvement over methods used in the past to control and account for material movement, proper software performance can only be assured through rigorous systems and software engineering practices.

While the above problems may be resolved through corrective actions associated with the recently submitted Implementation Plan for the Board's Recommendation 2002-1, *Quality Assurance for Safety-Related Software*, prudence dictates more urgent action. Therefore, pursuant to 42 U.S.C. §2286b(d), the Board requests that the National Nuclear Security Administration provide a report within 30 days of receipt of this letter that addresses the following topics:

- The actions being taken to improve SQA for the IEP system.
- The actions being taken to improve software quality for the Move Right system, including independent verification and validation efforts.

Sincerely,



John T. Conway
Chairman

c: The Honorable Everet H. Beckner
Mr. David E. Beck
Mr. Daniel E. Glenn
Mr. Mark B. Whitaker, Jr.