September 23, 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 been following closely the Department of Energy's (DOE) response to a reporting requirement dated January 20, 2000, which requested a corrective action plan to address deficiencies documented in the Board's technical report DNFSB/TECH-25, *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities*. Although more than two years have since elapsed, DOE has been unable to develop and execute an acceptable plan to resolve these issues, some of which were identified as early as 1989. Since the Board's August 15, 2001, public meeting on quality assurance, DOE has been developing an overall Quality Assurance Improvement Plan that includes software quality assurance as a key element, but this effort has not yet produced any substantial results.

As a result, the Board on September 23, 2002, unanimously approved Recommendation 2002-1, *Quality Assurance for Safety-Related Software,* which is enclosed for your consideration. After your receipt of this recommendation and as required by 42 U.S.C. § 2286d(a), the Board will promptly make it available for access by the public in DOE's regional public reading rooms. The Board believes that the recommendation contains no information that is classified or otherwise restricted. To the extent this recommendation does not include information restricted by DOE under the Atomic Energy Act of 1954, 42 U.S.C. §§ 216l-68, as amended, please see that it is promptly placed on file in your regional public reading rooms. The Board will also publish this recommendation in the *Federal Register*.

Sincerely,

John T. Conway
Chairman

c:  Mr. Mark B. Whitaker, Jr.
Enclosure

**DEFENSE NUCLEAR FACILITIES SAFETY BOARD**
**RECOMMENDATION 2002-1 TO THE SECRETARY OF ENERGY**
**Pursuant to 42 U.S.C. § 2286a(a)(5)**
**Atomic Energy Act of 1954, As Amended**

September 23, 2002

**Background.** Two core Integrated Safety Management (ISM) functions evolving from the Department of Energy's (DOE) implementation of Defense Nuclear Facilities Safety Board (Board) Recommendation 95-2, *Safety Management* are: (1) analyzing hazards; and (2) identifying and implementing controls to prevent and/or mitigate potential accidents. DOE relies heavily on computer software to analyze hazards, and design and operate controls that prevent or mitigate potential accidents.

DOE and its contractors use many codes to evaluate the consequences of potential accidents. Safety controls and their functional classifications are often based on these evaluations. Functional classifications establish the level of rigor to which controls are designed, procured, maintained, and inspected. The robustness and reliability of many structures, systems, and components (SSCs) throughout DOE's defense nuclear complex depend on the quality of the software used to analyze and to guide these decisions, the quality of the software used to design or develop controls, and proficiency in use of the software. In addition, software that performs safety-related functions in distributed control systems, supervisory control and data acquisition systems (SCADA), and programmable logic controllers (PLC) requires the same high quality needed to provide adequate protection for the public, the workers, and the environment. Other types of software, such as databases used in safety management activities, can also serve important safety functions and deserve a degree of quality assurance commensurate with their safety significance.

In some areas where there is at present no substantial activity in development of new software for safety applications, new calculations are usually based on existing codes, with data inputs and some logic chains often modified to fit the problems of the moment. It is therefore necessary to ensure that software so modified is not placed in general use in competition with generally validated and more widely useable software.

Software quality assurance (SQA) provides measures designed to ensure that computer software will perform its intended functions. Such measures must be applied during the design, testing, documentation, and subsequent use of the software, and must be maintained throughout the software life cycle. It is generally accepted that an effective SQA program ensures that:

All requirements, including the safety requirements, are properly specified.

! Models are a valid representation of the physical phenomena of interest, and digital control functions are properly executed.

! Input and embedded data are accurate.

! Software undergoes an appropriate verification and validation process.
! Results are in reasonable agreement with available benchmark data.

! All internal logic states of PLCs and SCADA are understood, so that no sequence of inputs, even those due to component failure, can leave the controlled system in an unexpected or unanalyzed state.

! Computer codes are properly and consistently executed by analysts.

! Code modifications and improvements are controlled, subjected to regression and re-acceptance testing, and documented.

DOE identified inadequate SQA as a problem as early as December 1989, when its Office of Environment, Safety and Health (DOE-EH) issued ENVIRONMENT, SAFETY & HEALTH BULLETIN EH-89-9, *Technical Software Quality Assurance Issues*. This bulletin states, "Inadequate SQA for scientific and technical codes at any phase in their 'life cycle' may not only result in lost time and/or excessive project costs, but may also endanger equipment and public or occupational sectors." The bulletin cites problems with all three types of software noted above (analysis, design, and operation). Likewise, a 1997 assessment performed by DOE's Accident Phenomenology and Consequence Assessment Methodology Evaluation Program determined that only a small fraction of accident analysis computer codes meet current industry SQA standards. SQA problems continue to persist, as documented in the Board's technical report DNFSB/TECH-25, *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities*, issued in January 2000.

An integrated and effective SQA infrastructure still does not exist within DOE. This situation can lead to both errors in technical output from software used in safety analyses and incorrect performance of instrumentation and controls for safety-related systems. In a letter to DOE dated January 20, 2000, the Board identified these deficiencies and requested that DOE provide a corrective action plan within 60 days. On October 3, 2000, the Board received DOE's corrective action plan, but found that it did not sufficiently respond to the Board's concerns. On October 23, 2000, the Board asked for a new plan of action; DOE has never submitted a revised plan, although several deliverables under the original plan have been received.

During the Board's August 15, 2001, public meeting on quality assurance, DOE proposed a revised set of actions to improve SQA processes and practices. Since then, DOE has attempted to develop a Quality Assurance Improvement Plan that includes SQA as a key goal. This action now appears stalled as a result of internal differences over objectives and funding. Thus, despite well over two years of effort, DOE has failed to develop and implement effective corrective actions in response to the Board's reporting requirement.

This situation is not acceptable. To improve SQA in the DOE complex, the Board recommends prompt actions to achieve the following:

*Responsibility and Authority*

1. Define responsibility and authority for the following: developing SQA guidance, conducting oversight of the development and use of software important to safety, and directing research and development as noted below. Roles and responsibilities should address all software important to safety, including, at a minimum, design software, instrumentation and control software, software for analysis of consequences of potential accidents, and other types of software, such as databases used for safety management functions.

2. Assign those responsibilities and authorities to offices/individuals with the necessary technical expertise.

*Recommended Computer Codes for Safety Analysis and Design*

3. Identify software that would be recommended for use in performing design and analyses of SSCs important to safety, and for analysis of expected consequences of potential accidents.

4. Identify an organization responsible for management of each of these software tools, including SQA, technical support, configuration management, training, notification to users of problems and fixes, and other official stewardship functions.

*Proposed Changes to the Directives System*

5. Establish requirements and guidance in the DOE directives system for a rigorous SQA process, including specific guidance on the following: grading of requirements according to safety significance and complexity; performance of safety reviews, including failure analysis and fault tolerance; performance of verification and validation testing; and training to ensure proficiency of users.

*Research and Development*

6. Identify evolving areas in software development in which additional research and development is needed to ensure software quality.