The Secretary of Energy
Washington, D.C.20585

February 5,2010

The Honorable John E. Mansfield
Vice Chairman
Defense Nuclear Facilities Safety Board
625 Indiana Avenue, NW, Suite 700
Washington, DC 20004-2901

Dear Mr. Vice Chairman:

On September 23,2002, the Defense Nuclear Facilities Safety Board (DNFSB) issued Recommendation 2002-1, *Quality Assurance for Safety Related Software*, to the Department of Energy (Department). Recommendation 2002-1 stated a concern regarding the lack of an integrated and effective quality assurance program for safety software and identified several actions that the Department needed to take to improve safety software quality assurance.

The Department submitted the Recommendation 2002-1 Implementation Plan (IP) to the DNFSB on March 13,2003. The IP defined the actions and processes that the Department would undertake and complete to enhance the quality of safety software used by the Department's defense nuclear facilities. Since then, the Department periodically informed the DNFSB of the completion of various commitments in the IP. The commitments with completion dates are identified in the enclosed report that describes the Department's ongoing effort in continuously improving safety software quality assurance. The report also addresses certain issues related to the control, grading, and use of consensus standards for safety software in departmental directives. These issues were noted during the October 15,2009, briefing to the DNFSB on the completion of the IP commitments.

The DNFSB's Recommendation 2002-1 has significantly improved safety software quality assurance within the Department. The Department will brief the DNFSB on the safety software quality assurance activities as requested, and as part of annual briefings on the quality assurance program implementation. The issues identified in the Recommendation have been addressed, therefore the Department requests formal closure of Recommendation 2002-1.

If you have any questions, please contact me or have your staff contact Mr. Andrew Lawrence, Director, Office Nuclear Safety, Quality Assurance and Environment at (202) 586-5680.

Sincerely,

Steven Chu

Enclosure

U. S. Department of Energy

Final Report to the Defense Nuclear Facilities Safety Board for Closure of Recommendation 2002-1, QualityAssurance for Safety Related Software

Washington, DC 20585

November 2009

1.0 Background

The Defense Nuclear Facilities Safety Board (DNFSB) issued Recommendation 2002-1, *Quality Assurance for Safety-Related Software,* on September 23,2002. In that Recommendation, the DNFSB recommended that the Department of Energy (DOE or Department) define specific responsibilities and authorities for safety software quality assurance (SSQA), and assign those responsibilities and authorities to individuals with the necessary technical expertise. The DNFSB also recommended that the Department identify and control design and analysis software, establish specific directives in the area of SSQA, and implement a continuous improvement process to maintain and upgrade software as necessary.

The Department accepted the DNFSB Recommendation on November 21,2002, and submitted its Implementation Plan (IP) for Recommendation 2002-1 to the DNFSB on March 13.2003. The IP defined the actions and urocesses that would be taken by the Department to ensure the quality of safety software at defense nuclear facilities. Safety software includes both safety system software and safety analysis and design software as defined in the IP. Actions outlined in the IP included:

- The identification, documentation and communication of roles, responsibilities and authorities for SSQA;
- The identification of Federal personnel in both Headquarters and the Field who have responsibility related to safety software along with competency requirements identified in a Technical Qualification Standard;
  An assessment of safety system software to determine its current status and an assessment of the effectiveness of SSQA programs for safety analysis and safety design software;
- The identification of a set of safety analysis "Toolbox" codes that are commonly used across the Department, the upgrade of those codes to a prescribed qualification, and the establishment of a Central Registry to facilitate maintenance, technical support, configuration management, and notification to users of problems and revisions to these codes;
  The identification and development of requirements and guidance for SSQA based on existing industry or Federal agency standards; and
- A continuous improvement process that includes the identification of SSQA experts across the Department to facilitate the sharing of information and lessons learned.

The overall execution of the Department's IP was the responsibility of the Office of Environment, Safety and Health (EH) and later the Office of Health, Safety and Security (HSS). However, responsibility for implementing software quality assurance rests with the Office of Environmental Management (EM) and the National Nuclear Security Administration (NNSA), and they provided many of the deliverables associated with commitments made within this IP.

2.0 Status of 2002-1 Implementation Plan Commitments

Attachment 1 provides a status summary of the commitments made in the IP, all of which are complete. Beginning June 20, 2003, periodic briefings were provided to the DNFSB and DNFSB staff. EM reported all of its commitments as completed on September 28, 2005, and NNSA reported all of its commitments as completed on November 3, 2006.

3.0 Activities to Ensure Safety Software Quality Assurance Program Effectiveness

The Department has undertaken multiple initiatives to implement the improvements outlined in the IP to ensure that continued attention is paid to the SSQA processes. Some examples of how SSQA has been institutionalized to date include:

- The Office of Quality Assurance Policy and Assistance (HS-23) was established with responsibility for SSQA;
- The DOE Federal Quality Council was established to promote quality assurance (QA) awareness across the DOE;
  The DOE EM/Office of Nuclear Energy/Office of Science Software Quality Assurance Support Group was established to promote software quality assurance (SQA) assistance to Federal staff;
- The Safety Software Expert Working Group was formed to provide technical support for reviewing Toolbox codes;
  Qualified SSQA staffing levels have increased;
- The Current QA directive DOE O 414.1C, Quality *Assurance* is being revised to enhance SSQA requirements;
- One new Toolbox code was added to the Central Registry, and two new code applications are under review; and
  The Safety Software Communication Forum is being developed to provide significant user interaction and enhanced capability and effective dissemination of information about safety software usage.

4.0 Review of Provisions for Safety Software in DOE Directives

In response to the DNFSB staff comments, the Department reviewed the following four SSQA issues as they pertain to the DOE directives.

4.1 Control of Safety Software Inventory

To ensure that safety software inventories are properly controlled, the Department plans to clarify existing requirements in the revision to DOE Order (O) 414.1C, Attachment 2, Contractor Requirements Document, Section 5.b. (2) and Attachment 5, Safety Software Quality Requirements for Nuclear Facilities, Section 2.b. (2).

This clarification sets forth an expectation that the site contractors control any addition, deletion, review, reconciliation, and approval of safety software in the inventory.

4.2 Risk Considerations in Safety Software Grading Criteria

DOE O 414.1C requires establishing and documenting grading levels for safety software using a graded approach as defined in the Order which references 10 Code of Federal Regulations (CFR) 830 Subpart A, *Quality Assurance*. The grading levels are further discussed DOE Guide (G) 414.1-4 which defines three grading levels (Level A, B or C) for safety software applications based on software failure and the impact on facility design and operation. Grading criteria consider the risk to the facility operation when software failures are postulated so that site contractors can determine and apply the appropriate grading level. The Guide utilizes the grading levels and the software types (custom developed, configurable, acquired, utility calculations, and commercial design and analysis tools) to recommend how the SQA work activities are applied. DOE O 414.1C is being revised to include approval requirements for the grading levels.

4.3 Grading Safety Software Quality Assurance Work Activities

SQA work activities are implemented based upon the graded level of the safety software and the applicable software type. DOE G 414.1-4, *Safety Software Guide*, Section 5.2, Table 4 provides a summary of the mapping between safety software type, the grading levels, and the ten SQA work activities. Depending on the grading level of safety software (Level A, B or C), all work activities may not be applicable for a particular type of safety software. The Guide indicates when each work activity may applicable (fully or graded) or omitted. In Table 4, the term "Full" implies that a full consideration of the applicable provisions of the selected consensus standard is necessary for the particular SSQA work activity. The term "Grade" indicates that a graded approach following the criteria defined in DOE O 414.1C may be applied for the work activity. The term "n/a" indicates that the work activity is not applicable. Sections 5.2.1 through 5.2.10 provide the rationale and other considerations for applying the "Full", "Grade" or "n/a" designation in Table 4 for each safety software type and SQA work activity. Applying a graded approach requires engineering judgment with respect to the levels of analysis, documentation and actions to be applied.

4.4 Adoption of a Comprehensive Consensus Standard

DOE O 414.1C, *Quality Assurance* is being revised to incorporate the experience gained in the application of the Order since it was issued in June 2005. The provisions of revision to DOE O 414.1C promotes the use

of American Society of Mechanical Engineers NQA-1-2000 or 2008 including appropriate Addenda (or a later edition), *Quality Assurance Requirements for Nuclear Facility Application,* **Part** *I* and requirements of Part II, Subpart 2.7.

5.0 Basis for Closure of Recommendation 2002-1

The issues identified in Recommendation 2002-1 have been addressed and the basis to support closure exists.

- The Department's IP for Recommendation 2002-1 has significantly improved SSQA;
- The objectives identified in the IP have been achieved;
- All IP commitments have been completed; and
- SSQA processes are functioning and are driving continuous improvement.

Attachment 1: Status of 2002-1 Implementation Plan Commitments

Number	Commitment	Status
4.1.1	Issue a DOE Notice that identifies, documents, and communicates roles, responsibilities, and authorities for SQA by organizational element.	**Complete.** DOE Notice 411.1, *Safety Software Quality Assurance Functions, Responsibilities, and Authorities for Nuclear Facilities and Activities* issued August 27, 2003.
4.1.2	Establish technical qualification requirements for Federal personnel whose duties and responsibilities require them to provide assistance, guidance, direction, oversight, or evaluation of safety software QA activities.	**Complete.** *Safety Software Quality Assurance Functional Area Qualification Standard,* DOE-STD-1172-2003 issued in the Technical Standards Program in December 2003.
4.1.3	Identify the Federal positions whose duties and responsibilities require them to provide assistance, guidance, direction, oversight, or evaluation of safety software QA activities.	**Complete.** EM list of TQP positions updated to include SQA was provided to the DNFSB January 29,2004. NNSA list of TQP positions updated to include SQA was provided to the DNFSB on December 9,2003.
4.1.4	Personnel assigned to SQA positions achieve qualification per the requirements of the Technical Qualification Program (TQP).	**Complete.** EM status report of personnel qualified to SQA positions was provided to DNFSB November 29,2004. NNSA status report of personnel qualified to SQA positions was provided to the DNFSB on July 25,2005.
4.1.5	Revise the Functions, Responsibilities and Authorities Manual (FRAM) to incorporate Federal responsibility and authority for SQA.	**Complete.** FRAM revised to incorporate Federal responsibility and authority for SQA and provided to the DNFSB on December 31,2003.
4.1.6	Revise the Headquarters and field element Functions, Responsibilities and Authorities (FRA) documents to incorporate Federal responsibilities and authorities for SQA.	**Complete.** EM FRA revised to incorporate Federal responsibilities and authorities for SQA and provided to the DNFSB on May 6,2004. NNSA FRA revised to incorporate Federal responsibilities and authorities for SQA and provided to the DNFSB on September 9,2005. Los Alamos Site Office (LASO) update provided to DNFSB on April 10,2006.

Number	Commitment	Status
4.2.1.1	Identify the codes used for safety analysis to be part of the Safety Analysis Code Toolbox.	Complete. Identified as complete when the Implementation Plan was issued. Initial list of six codes identified based on detailed survey conducted by Safety Analysis Software group. Results in report titled Selection of Computer Codes for DOE Safety Analysis Applications. Memorandum sent from EH to EM and NNSA on March 28, 2003, designating Toolbox codes.
4.2.1.2	Establish SQA criteria for the safety analysis Toolbox codes.	Complete. SQA plan and criteria for the Toolbox codes were developed and provided to the DNFSB on September 30,2003, and are available on Central Registry web site at http://www.hss.doe.gov/CSA/CSP/sqa/central_registry.htm
4.2.1.3	Perform a gap analysis on the Toolbox codes to determine the actions needed to bring the code into compliance with SQA qualification criteria and develop a schedule with milestones to upgrade each code based on the gap analysis results.	Complete. Gap analysis reports were developed for the six Toolbox codes and provided to the DNFSB on May 12,2004 and are available on Central Registry web site at http://www.hss.doe.gov/CSA/CSP/sqa/central_registry.htm.
4.2.1.4	Issue code-soecific guidance reports on use of the "Toolbox" codes identifying applicable regimes in accident analysis, default inputs, and special conditions for use.	Complete. Code-specific guidance reports were developed on the use of safety analysis Toolbox codes identifying applicable regimes in accident analysis, default inputs, and special conditions for use. Code guidance reports for the six Toolbox codes were provided to the DNFSB on June 29, 2004, and are available on Central Registry web site at http://www.hss.doe.gov/CSA/CSP/sqa/central_registry.htm
4.2.1.5	Conduct a survey of design codes currently in use to determine if any should be included as part of the Toolbox codes.	**Complete.** Survey of design codes was conducted and the report documenting the survey results was provided to the DNFSB on January 29, 2004, and is available on Central Registry web site at http://www.hss.doe.gov/CSA/CSP/sqa/central_registry.htm
4.2.2	Establish and implement a Central Registry for the long-term maintenance and control of the safety analysis Toolbox codes.	Complete. Memorandum from the Deputy Secretary establishing the Central Registry provided to the DNFSB on August 29,2003.

Number	Commitment	Status
4.2.3.1	Develop criteria and guidance for the identification, selection and assessment of safety system software and firmware at defense nuclear facilities.	**Complete.** Criteria review and approach document (CRAD) was developed for the identification, selection and assessment of safety system software and firmware at defense nuclear facilities and was provided to the DNFSB on October 28, 2003. Available on Central Registry web site at http://www.hss.doe.gov/CSA/CSP/sqa/central_registry.htm
4.2.3.2	Establish a schedule to complete the identification, selection, and assessments of safety system software and firmware at defense nuclear facilities.	**Complete.** NNSA schedule of assessments was provided to the DNFSB on December 22, 2003. EM schedule of assessments was provided to the DNFSB on January 29, 2004.
4.2.3.3	Complete the identification, selection, and assessments of safety system software and firmware at defense nuclear facilities.	**Complete.** EM assessments completed and provided to the DNFSB on December 29, 2004. NNSA assessments completed and provided to DNFSB on July 28, 2005.
4.2.4.1	Develop criteria and guidance to assess that the processes in place to ensure that safety software currently used to support the analysis and design of defense nuclear facilities are adequate.	**Complete.** A CRAD was developed to assess that the processes in place to ensure that safety software currently used to support the analysis and design of defense nuclear facilities are adequate and provided to the DNFSB on October 28, 2003. Available on Central Registry web site at http://www.hss.doe.gov/CSA/CSP/sqa/central_registry.htm
4.2.4.2	Establish a schedule to complete the assessment of the processes in place to ensure that safety software currently used to support the analysis and design of defense nuclear facilities are adequate.	**Complete.** NNSA schedule of assessments was provided to the DNFSB on December 22, 2003. EM schedule of assessments was provided to the DNFSB on January 29, 2004.
4.2.4.3	Complete the assessments of the processes in place to ensure that safety software currently used to support the analysis and design of defense nuclear facilities is adequate.	**Complete.** EM assessments completed and provided to DNFSB October 1, 2004. NNSA assessments completed and provided to the DNFSB on July 28, 2005.

Number	Commitment	Status
4.3.1	Conduct a review to identify the industry or Federal agency standards that are appropriate for DOE safety software.	**Complete.** Report identifying appropriate industry or Federal agency standards that are appropriate for DOE safety software developed and provided to the DNFSB on September 30.2003. Available on Central Registry web site at http://www.hss.doe.gov/CSA/CSP/sqa/central_registry.htm
4.3.2.1	Establish a schedule to develop, revise, approve, and issue required SQA directives.	**Complete.** Schedule to develop, revise, approve, and issue required SQA directives was provided to DNFSB October 31, 2003. Status reports were provided to the DNFSB on February 28, 2005, and February 26,2008.
4.3.2.2	Issue required SQA directives.	Complete. DOE O 414.1C and DOE G 414.1-4 were issued June 17,2005.
4.3.3	Headquarters and Field Elements review the approved SQA directives and determine the actions necessary to implement the requirements.	Complete. EM provided its SQA directive Implementation Plan and schedule to the DNFSB September 28,2005. NNSA provided its SQA directive Implementation Plan and schedule to the DNFSB on November 3,2006.
4.4.1	Establish a corporate QA function within EH that is responsible and accountable for the identification and resolution of Departmental crosscutting QA issues, such as SQA.	**Complete.** DOE O 414.1C revised to incorporate EH's QA and SQA roles and responsibilities June 17,2065. The DNFSB was notified on June 29,2005.
4.4.2	Identify methods for capturing and clearly communicating SQA lessons learned, new technology, innovative techniques, and areas in software development in which research and development is needed to ensure software quality.	Complete. Information sharing mechanism for SQA established and provided to the DNFSB on October 31,2003.

Number	Commitment	Status
4.4.3	Establish relationships and actively participate with outside groups, organizations, companies, and agencies that have an interest in SQA similar to that being addressed by this IP. This participation will assist the Department in benchmarking, research and development, and sharing of lessons learned and new technologies.	**Complete.** Report describing relationships with outside groups including points of- contact provided to the DNFSB on December 18,2003.
5.2.1	The Department will provide briefings to the DNFSB and DNFSB Staff. These briefings will include updates on the status of completing actions identified in the various reviews and assessments indicated in this IP.	**Complete.** Beginning June 20, 2003, periodic briefings have been provided to the DNFSB and DNFSB staff. QA and SQA briefings are now combined.