Department of Energy
Washington, DC 20585

February 7, 2008

The Honorable A.J. Eggenberger
Chairman
Defense Nuclear Facilities Safety Board
625 Indiana Avenue, NW, Suite 700
Washington, DC 20004-2901

Dear Dr. Eggenberger:

In the Department's quality assurance briefing to the Defense Nuclear Facilities Safety Board (DNFSB) on October 4, 2007, my staff committed to develop an approach and schedule by the end of 2007 for further addressing residual actions associated with Commitment 4.2.1.3 of the Department's Implementation Plan for DNFSB Recommendation 2002-1, *Quality Assurance for Safety Related Software.* This commitment required the Department to perform a gap analysis on the six original toolbox codes to determine the actions needed to bring the codes into compliance with Software Quality Assurance criteria.

The gap analysis reports for each of the original six toolbox codes have been completed. The gap analysis reports concluded that no software induced errors existed in the codes that would have led to non-conservatism at defense nuclear facilities. Additionally, code-specific guidance reports were issued to assist code users in the application of the toolbox codes. However, follow-up actions to resolve the gaps for each code based on the gap analysis have not been completed.

The attached path forward includes a plan and schedule outlining what has been accomplished to date along with the approach that will be used to resolve the gaps identified in the toolbox code gap analysis reports to allow closure of DNFSB Recommendation 2002-1. This plan and schedule, which has been jointly developed with the Office of Environmental Management and the National Nuclear Security Administration, have been discussed with members of your staff.

In the Department's October 4, 2007, quality assurance briefing, my staff also committed to provide a separate submittal in the second quarter of calendar year 2008, describing how the Safety Software Central Registry will be managed including code version changes and adding, as necessary, new codes such as safety design codes. The experience gained from working with the toolbox code developers during the gap closure effort, together with additional information regarding code usage from code users, will be used to develop a strategy for managing the Central Registry that will be productive and cost effective for the

Department. If you have any questions, please contact me at (301) 903-3777 or your staff may contact Charles Lewis, Acting Director, Office of Corporate Safety Analysis, at (301) 903-8008 or Subir Sen, Office of Corporate Safety Programs, at (301) 903-6571.

Sincerely,

Glenn S. Podonsky
Chief Health, Safety and Security Officer
Office of Health, Safety and Security

Attachment: Path Forward to Address Gaps in Toolbox Code Gap Analysis Reports

PATH FORWARD TO ADDRESS GAPS IN TOOLBOX CODE GAP ANALYSIS REPORTS

Department of Energy
Office of Health, Safety and Security
Office of Environmental Management
National Nuclear Security Administration

Table of Contents

PATH FORWARD TO ADDRESS GAPS IN TOOLBOX CODE GAP ANALYSIS REPORTS

Introduction

Six toolbox codes were added to the Safety Software Central Registry as part of the Department's Implementation Plan (IP) for Defense Nuclear Facilities Safety Board (DNFSB) Recommendation 2002-1 *Quality Assurance for Safety Related Software.* IP commitment 4.2.1.3 required the Department to perform a gap analysis on the six original toolbox codes to determine the actions needed to bring the codes into compliance with Software Quality Assurance (SQA) criteria. A gap analysis was conducted for each of the six toolbox codes and the actions needed to bring the codes into compliance with SQA criteria have been identified.

The gap analysis was based on a set of SQA requirements and criteria generally compliant with American Society of Mechanical Engineers (ASME) Nuclear Quality Assurance (NQA)-1-2000, *Quality Assurance Requirements for Nuclear Facility Applications.* Each toolbox code was evaluated against ten SQA criteria/requirements. Summary conclusions for each code based on the ten SQA criteria/requirements are contained in Section 5.0 of the respective gap analysis report.

The six toolbox codes are considered safety analysis software per the definition in Department of Energy (DOE) O 414.1C, *Quality Assurance.*

Previous Activities

The Office of Health, Safety and Security (HSS) is responsible for maintaining the Department's Safety Software Central Registry which contains the six toolbox codes used by nuclear facility contractors along with the gap analysis reports and code guidance reports for each toolbox code. Since the gap analysis reports were completed for the toolbox codes in May 2004, and because the Department does not own the six current toolbox codes, the code owners were contacted to determine the schedule, level of effort and cost required to address the identified gaps for each code.

Early discussions with the code owners/developers did not produce the desired results. This was due in part to: (1) The DOE does not own the codes, (2) code owners/developers did not appreciate the need to address the new SQA requirements, and (3) the cost involved in addressing all of the gaps could be substantial.

In June 2005, DOE O 414.1C, *Quality Assurance* and DOE G 414.1-4, *Safety Software Guide* were issued which require the use of NQA-1-2000 or other national or international consensus standards with similar quality requirements for SQA work activities. These were the first DOE directives to identify and define specific SQA requirements which are based on NQA-1-2000. This played a large part in making the

DOE complex aware of SQA requirements. As a result, site contracts have been revised to incorporate DOE O 414.1C and site SQA programs are being developed to address SQA requirements.

Proposed Approach

A. Application of NQA-1 Criteria

The toolbox code gap analysis performed in 2004 was conducted using a ten point criteria to define and evaluate the software life cycle activities related to: (1) Software Classification; (2) SQA Procedures and Plans; (3) Requirement Phase; (4) Design Phase; documentation; (5) Implementation Phase; (6) Testing Phase; (7) User instructions; (8) Acceptance Test; (9) Configurations Control; and (10) Error Impact.

The ten-point criteria was not in existence at the time the six toolbox codes were developed and issued for use. As a result, the toolbox codes do not meet many of these system development life cycle criteria. However, NQA-1-2000, Subpart 2.7, Section 302 provides specific requirements for accepting "acquired" software that were previously approved under a program which is not consistent with NQA-1-2000. The specific code section sates that:

"Software that has not been previously approved under a program consistent with this Standard for use in its intended application (e.g., freeware, shareware, procured commercial off-the-shelf, or otherwise acquired software) shall be evaluated in accordance with the requirements of this Subpart. The software shall be identified and controlled prior to evaluation. The evaluation, specified by this section, shall be performed and documented to determine adequacy to support operation and maintenance and identify the activities to be performed and the documentation that is needed.

This determination shall be documented and shall identify as a minimum

- *(a) capabilities and limitations for intended use*
- *(b) test plans and test cases required to demonstrate the capabilities within the limitations*
- *(c) instructions for use within the limits of the capabilities*

Exceptions from the documentation requirements of this Subpart and the justification for acceptance shall be documented.

The results of the above evaluation and the performance of the actions necessary to accept the software shall be reviewed and approved. The resulting documentation and associated computer program(s) shall establish the current baseline.

Revisions to previously baseline software received from organizations not required to follow this Subpart shall be evaluated in accordance with this section."

The six toolbox codes meet the NQA-1-2000 definition "acquired" software because the Department does not own the toolbox codes and the toolbox codes were either developed at the direction of and/or with funding from other government agencies or they are privately owned. Using the NQA-1-2000, Section 302, Subpart 2.7 criteria and mapping them against the ten-point criteria used in the gap analysis, indicates that the Section 302 criteria are adequately satisfied by the criteria 6 through 10 of the gap analysis reports. The emphasis here is on well documented reference and user manual, code validation, configuration control and error reporting and corrective action.

Further review of the 2004 gap analysis documents revealed that some of the reported deficiencies pertaining to several sub-elements of the criteria 6 through 10 were attributed, for example, to lack of explicit documentation pertaining to criteria 2 through 5, or documentation not available during the gap analysis effort. Of the ten criteria, number 1 is a determination made by the code user and the criteria 2 through 5 are normally performed before the software is issued for general use.

Based on the above discussion of the application of NQA-1-2000 criteria, the Department will:

- review of the gap analysis results for criteria 6 through 10 for each of the toolbox codes by knowledgeable code practitioners and develop an approach to address the gaps and,
- follow-up with the code developers/owners to resolve the gaps which must be addressed to comply with the NQA-1-2000.

B. Gap Analysis Review

A team of knowledgeable code users will be assembled to review individual gap analysis reports and using expert judgment categorize the suggested gap analysis report recommendations as follows:

1. Identify those gaps that have been addressed with the issuance of a later revision to the toolbox code.
2. Identify and prioritize the gaps that should be implemented as part of the code documentation/procedure upgrade.

The resolution of these gaps will further address the residual actions associated with IP Commitment 4.2.1.3.

C. Code Developer Input

All six toolbox code developers/owners/responsible entity have been contacted and briefed on the results of the gap analysis report and a path forward to address bringing the codes into compliance with NQA-1-2000 criteria. Discussions with the code developers/ owners revealed that some of the documentation and procedure related issues in the gap analysis reports can be resolved by other existing documents/procedures which have been put in place since the gap analyses were conducted or are being planned. The code

developers are generally receptive in helping to resolve the outstanding gap analysis issues but have funding constraints.

D. Management of the Central Registry

A strategy for managing the Safety Software Central Registry including code version changes and adding new codes, as necessary, such as safety design codes will be developed. The experience gained working with the toolbox code developers during the gap closure effort together with the additional information to be gathered regarding code usage from the code users will be used in part to develop a strategy that will be productive and cost effective for the Department.

Action Plan and Schedule

This action plan and schedule has been developed jointly by HSS, the Office of Environmental Management (EM) and the National Nuclear Security Administration (NNSA). HSS will take the lead in these activities with EM and NNSA actively participating in terms of reviews, data gathering, resources, and interaction with the DNFSB.

Table 1 provides a summary of current toolbox code gap closure status. The following actions will be undertaken collaboratively by HSS, EM, and NNSA to resolve the gaps for each code based on the gap analysis reports.

Activity	Estimated Completion Date
1. Establish the evaluation Team and the necessary funding for activities.	March 2008
2. Review the gap analysis reports for each toolbox code and develop a closure plan consistent with the proposed approach.	May 2008
3. Develop Safety Software Central Registry management strategy.	June 2008
4. Implement the closure plan with each toolbox code developer to address the gaps.	September 2008
5. Develop addendum to the gap analysis reports as needed.	November 2008
6. Brief DNFSB staff on progress in implementing the Action Plan.	As Necessary
7. Complete the actions to address gaps identified in gap analysis reports.	December 2008

Upon completion of this review procedure, it is possible that a timely and cost effective resolution of all the gap analysis report issues may not be feasible. HSS may then provide additional guidance as necessary regarding the unresolved gaps.

Table 1
Toolbox Code Gap Closure Status

Toolbox Code	Gap Closure Status	Owner/ Developer
CFAST	In progress via code upgrade by code developer	NIST
GENII	Gap to be addressed by code developer	EPA/PNL
EPI	In progress by code developer	Homann Associates
MELCOR	Under review by SNL/Gaps to be addressed by code developer	NRC/SNL
MACCS2	Under review by SNL/Gaps to be addressed by code developer	NRC/SNL
ALOHA	Multi-year project by code developer to address gaps.	EPA/NOAA

Note: Code Owner/Developer
EPA: Environmental Protection Agency
NIST: National Institute of Science and Technology
NOAA: National Oceanic and Atmospheric Agency
NRC: Nuclear Regulatory Commission
PNL: Pacific National laboratory
SNL: Sandia national Laboratory