Department of Energy
Washington, DC 20585

December 22, 2008

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

Dear Mr. Chairman:

In the Department of Energy's (DOE) quality assurance briefing to the Defense Nuclear Facilities Safety Board on June 25, 2008, my staff made a presentation on the status of the DOE Central Registry and the actions being considered to update existing toolbox codes to newer code versions and to add new codes to the Central Registry. The attached Safety Software Central Registry and Communication Portal Management Plan, which has been developed jointly with the Office of Environmental Management and the National Nuclear Security Administration, further describes DOE's approach for managing the safety software Central Registry.

Questions may be directed to me at (301) 903-3777 or your staff may contact Andrew Lawrence, Director, Office of Nuclear Safety, Quality Assurance, and Environment at (202) 586-5680.

Sincerely,

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

Enclosure

SAFETY SOFTWARE CENTRAL REGISTRY AND COMMUNICATION PORTAL MANAGEMENT PLAN

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

December 2008

Table of Contents

1.0 Introduction

As part of Department of Energy's (DOE) efforts to continuously improve the management of the Safety Software Central Registry, DOE provides updates describing how the Central Registry is being managed, including updating existing toolbox codes to newer code versions and adding new codes to the Central Registry. The Office of Health, Safety and Security (HSS) worked with the Office of Environmental Management (EM) and the National Nuclear Security Administration (NNSA) collaboratively to develop DOE's Safety Software Central Registry and Communication Portal Management Plan.

2.0 Background

The Safety Software Central Registry is made up of toolbox codes that meet the definition of safety and hazard analysis software and design software, and that have been appropriately qualified per the DOE Order (O) 414.1C, *Quality Assurance,* safety software quality assurance (SSQA) requirements. Safety software as defined in DOE O 414.1C includes: safety system software, safety and hazard analysis software, design software and safety management and administrative controls software. For a complete definition of safety software, see the Appendix. Six toolbox codes[1] were originally included in the Central Registry as part of DOE's Implementation Plan for the Defense Nuclear Facilities Safety Board (DNFSB) Recommendation 2002-1, *Quality Assurance for Safety Related Software.* A seventh code, Integrated Modules for Bioassay (IMBA) Expert DOE Edition V 4.0.28, was later added. Prior to inclusion in the Central Registry, an evaluation was conducted for each toolbox code to identify any "gaps" between the software quality assurance (SQA) pedigree of the specific code and DOE requirements for safety software. Code-specific guidance reports were also developed to identify applicable regimes in accident analysis, default inputs, and special conditions for using the toolbox codes. These documents are available for each toolbox code on the Central Registry Website. Two other codes, IMBA Professional Plus (newer version of IMBA) and Hotspot, were reviewed for inclusion in the Central Registry, and the code developers for these codes are in the process of implementing the review recommendations to allow for their inclusion in the Central Registry.

On February 7, 2008, the Department submitted to the DNFSB the *Path Forward to Address Gaps in Toolbox Codes Gap Analysis Reports* regarding the original six toolbox codes. The path forward is currently being implemented and includes two important components: 1) the formation of the Safety Software Expert Working Group (SSEWG), and 2) the conduct of safety analysis and design code data call. Both of these components will be used in the implementation of this Management Plan.

DOE's Implementation Plan for DNFSB Recommendation 2002-1 also required that a safety design code survey be conducted to determine if additional codes should be added to the Central Registry. The survey was completed in Fiscal Year 2003 (FY03) and found that most of the safety design codes being used are proprietary. The survey results identify approximately 70

[1] ALOHA V5.2.3, CFAST V3.1.7 and 5.0.1, EPI code V7.0, GENII 1.485 and V2.0, MACCS2 V1.13.1, and MELCOR 1.85

codes in the safety design arena. These codes are used in multiple industries outside of the DOE with most being widely distributed and used for multiple applications. Based on these specific characteristics of the design codes, it was concluded in the survey report that existing SQA for the safety design codes was adequate and no safety design codes were recommended for inclusion into the Central Registry.

The toolbox codes do not actually reside in the Central Registry as these codes were developed and are under the control of entities outside of DOE (e.g., other Federal agencies or the private sector). Access to the toolbox codes or their use is subject to agreements, conditions and restrictions established by the code owners or Federal agencies. The toolbox code owners are responsible for ensuring that the codes are maintained in accordance with established requirements.

Use of the Central Registry toolbox codes is not mandatory. However, using the codes offers a number of advantages to the DOE and its contractors. Some of these advantages include: 1) the gap analysis evaluation performed provides valuable information on the code regarding application of SQA requirements; 2) the evaluation extends beyond the DOE safety software quality assurance criteria to review the code's capability to properly perform safety basis calculations; 3) DOE specific guidance documents identify limitations and vulnerabilities not readily found in other code documentation are available; 4) due to the established pedigree, assessments of the toolbox code by DOE field offices and site contractors may be reduced in scope; and 5) the ability to monitor and communicate to DOE users information on code features and resolutions to defects.

3.0 Objective

The objective of this Safety Software Central Registry and Communication Portal Management Plan is to outline the approach for managing the Central Registry (including code version changes, and adding or removing codes), as well as to provide a mechanism for communicating with the users.

Since the Department's Implementation Plan for DNFSB Recommendation 2002-1 was developed, and DOE O 414.1C and DOE Guide (G) 414.1-4 were issued in 2005, the need for a more comprehensive approach to the management of the Central Registry has become apparent due to the following:

- The Central Registry refers to specific versions of the toolbox codes. Over time, these codes have been updated and the newer versions have not been evaluated for inclusion in the Central Registry.
- There is increased awareness of SQA requirements in the DOE complex, resulting in new requests for codes to be evaluated for inclusion in the Central Registry.
- Site contractors are taking the initiative to qualify codes (not in the Central Registry) to the DOE SQA requirements, creating an opportunity to leverage these activities and evaluate the codes for inclusion in the Central Registry.
- The Department conducted a survey of the safety design codes in FY03 and came to the conclusion that the safety design codes need not be included in the Central Registry.

However, due to the dynamic nature of the software industry and application of these codes in new projects across DOE, an updated data call on the use of safety analysis and design codes was deemed prudent. This will provide a better understanding of the safety and hazard analysis software and design software currently in use at DOE, thereby facilitating a new review of these codes for inclusion in the Central Registry.

- The need exists for a centralized communication platform where DOE and contractor personnel can access information on safety and hazard analysis software and design software in use across the DOE complex and exchange information on proper use of these codes.

Therefore, a comprehensive and integrated approach is needed to improve management of the Central Registry and associated functions to promote continuous improvement in the application of SQA and the use of safety and hazard analysis software and design software at DOE.

4.0 Management of Safety Software in the Central Registry

The process for managing the Central Registry will be implemented consistent with DOE G 414.1-4. HSS is responsible for the management of the Central Registry. HSS, EM, and NNSA worked collaboratively in the development of this Management Plan and will continue to work together in the implementation of the Management Plan.

For effective management of the Central Registry, it is essential to assemble a group of experienced code users with intimate knowledge of the theory and operation of the codes. The SSEWG will constitute such a group and will provide expert advice and serve as a resource for the management of certain functions of the Central Registry. The SSWEG members will generally be chosen from DOE and contractor staff and will initially support activities related to the original six toolbox codes. The group will be expanded to support the code-specific independent evaluations referenced in 4.1 and 4.3.

Managing the Central Registry consists of the following elements:

- Updating the Inventory of Central Registry Toolbox codes
- Adding new codes suggested by software sponsors
- Leveraging site contractor SSQA activities

4.1 Updating the Inventory of Central Registry Toolbox Codes

Since the inception of the Central Registry, the toolbox codes have been revised and more revisions can be anticipated. Therefore, it is important to establish a cost-effective way, based on need, for updating the existing toolbox codes to newer versions. DOE will work closely with the developers to obtain the documentation to support an independent evaluation of the code per DOE G 414.1-4. The SSEWG will be a resource for performing the independent evaluation.

4.2 Adding New Codes to the Central Registry

Adding new codes to the Central Registry will require a software sponsor and an SQA Evaluator. The sponsor is either the originator of the software (developer) or a primary user (site organization) which is requesting the software to be included in the Central Registry. The software sponsor is responsible for documenting the rationale and developing the review documents (per DOE G 414.1-4) for adding the software to the Central Registry.

In general, the rationale for adding safety and hazard analysis software and design software to the Central Registry should include evidence that: 1) there is widespread use of the software across DOE complex for safety-related applications; 2) proper software information, error configuration control, and other SQA requirements can be met; and 3) a benefit exists for adding the software to the Central Registry. The sponsor is also responsible for designating the SQA Evaluator to conduct the independent review.

The SQA Evaluator (individual or team) is an independent reviewer of the computer software and is not affiliated with the software developing organization. The SQA Evaluator is responsible for documenting the SQA evaluation, confirming that the software SQA satisfactorily meets the requirements for inclusion to the Central Registry.

The Office of Quality Assurance Policy and Assistance approves the SQA Evaluator designated by the software sponsor and reviews the software evaluation. HSS will determine whether the software should be included in the Central Registry.

IMBA Professional Plus and Hotspot are two codes that have been evaluated based on DOE G 414.1-4 and the code developers are in the process of responding to critical recommendations from DOE.

4.3 Leveraging Site Contractor SSQA Activities

For safety and hazard analysis software and design software codes, (where the DOE site contractor(s) have approved use of a code per Appendix B of DOE G 414.1-4.) HSS, with the help of the line organization, will identify candidate safety and hazard analysis software and design software code(s) and review the rationale for inclusion in the Central Registry. If the decision is to consider the proposed code for inclusion in the Central Registry, the process outlined in Appendix B of DOE G 414.1-4 is to be followed.

5.0 Safety Software Communication Portal

To allow the DOE safety and hazard analysis software and design software code users to effectively communicate with one another by sharing experiences and obtaining information on the use of the codes, HSS, EM, and NNSA are developing a web-based Communication Portal. The portal will include a Communication Forum and a Safety Software Usage Catalog.

5.1 Communication Forum

The Communication Forum will be used to promote continuous improvement and sharing of information and knowledge of safety and hazard analysis software and design software. The Communication Forum will be a password protected system that consolidates usage information and will contain links to experienced code users, procedures, training information, good practices and lessons learned, as well as a discussion forum to address user issues.

The Communication Forum will provide a platform for communicating information about various safety and hazard analysis software and design software codes used at DOE sites. From the Central Registry website, registered users will be able to:

- view an updated catalog of safety software used at their site
- view safety and hazard analysis software and design software code usage information at sites across DOE
- access links to the code developers' websites
- participate in the Discussion Forum

The Communication Forum will also allow users to exchange information about the usage of individual safety and hazard analysis software and design software codes, submit information on problems, and submit general information or suggestions on the use of individual codes. Users will be able to review submittals based on several criteria and to respond to inquiries.

5.2 Safety Software Usage Catalog

A safety analysis and safety design code data call is being conducted to gather code usage information on the existing Central Registry toolbox codes as well as other safety and hazard analysis software and design software currently used by EM and NNSA site contractors. Information requested includes:

- code version number
- whether designated as safety and hazard analysis software and design software per DOE O 414.1C
- whether supporting SQA documentation exist for codes designated as safety and hazard analysis software and design software
- whether the code is considered proprietary
- frequency of use: occasional or frequently
- whether errors are reported to code developers
- if code developers notify the users of errors
- existence of a configuration control process
- code user point-of-contact information

The safety software usage catalog including code user point-of-contact information, will be developed from the above information and will be displayed on the Communication Forum. To be included in the catalog, codes must meet the definition of safety and hazard analysis software and design software (see Appendix).

Maintenance of the safety software code usage catalog will be performed through the Communication Forum. This will provide a baseline of safety and hazard analysis software and design software. This can then be updated by individuals designated by site management, using the website access, to keep the information current. The information on the website is available to users in several reporting formats.

HSS, with assistance from EM, NNSA and the SSEWG, will review the responses from the safety analysis and safety design code data call and evaluate the need to include any safety design codes in the Central Registry. Any safety design code recommended for inclusion is to follow the process outlined in Appendix B of DOE G 414.1-4.

Note: The safety software usage catalog is a list of codes in use that meet the definition of safety and hazard analysis software and design software. This does not mean that these codes and/or code versions have been designated as Central Registry toolbox codes. The current inventory of Central Registry toolbox codes can be found at http://www.hss.energy.gov/csa/csp/sqa/central_registry.htm. It is the code users' responsibility to verify that, prior to using codes/versions not specifically cited in the Central Registry, the code/version meets the SSQA requirements. Additionally, all other QA requirements pertaining to local installation of codes should be met.

Appendix

Glossary

1. **Central Registry:** An information repository designated to contain the inventory of the Department's safety software toolbox codes including code-specific gap analysis documents, guidance documents, and contact information.

2. **SSEWG:** A group of experienced code users with intimate knowledge of the theory and operation of various codes. These individuals have used the codes often and have thorough familiarity with available code specific user's manual, reference manual, and verification and validation report.

3. **Safety Software (definition per DOE O 414.1C):** Safety Software includes the following types of software:

   a) Safety System Software: Software for a nuclear facility that performs a safety function as part of a structure, system, or component and is cited in either: 1) a DOE approved documented safety analysis, or 2) an approved hazard analysis per DOE P 450.4, *Safety Management System Policy,* dated 10-15-96, and the DEAR clause.

   b) Safety and Hazard Analysis Software and Design Software: Software that is used to classify, design, or analyze nuclear facilities. This software is not part of a structure, system, or component but helps to ensure the proper accident or hazards analysis of nuclear facilities or an SSC that performs a safety function.

   c) Safety Management and Administrative Controls Software: Software that performs a hazard control function in support of nuclear facility or radiological safety management programs or technical safety requirements, or other software that performs a control function necessary to provide adequate protection from nuclear facility or radiological hazards. This software supports eliminating, limiting, or mitigating nuclear hazards to workers, the public, or the environment as addressed in 10 CFR 830, 10 CFR 835 and the DEAR ISMS clause.

4. **Toolbox Codes:** A set of qualified computer codes, by version release, listed in the DOE Safety Software Central Registry that are routinely and widely used in DOE to support safety analyses. These codes may also include commercial or proprietary design codes where DOE considers additional SQA controls are appropriate and beneficial.